

ProSecure Web/Email Security Threat Management Appliance STM150/300/600 Reference Manual



NETGEAR®

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134

202-10519-01
1.0
September 2009

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks and ProSecure is a trademark of NETGEAR, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by NETGEAR could void the user's authority to operate the equipment.

EU Regulatory Compliance Statement

The ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600 is compliant with the following EU Council Directives: EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC. Compliance is verified by testing to the following standards: EN55022, EN55024, and EN60950-1.

For the EU Declaration of Conformity please visit:
http://kb.netgear.com/app/answers/detail/a_id/11621/sno/0.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Additional Copyrights

AES	Copyright (c) 2001, Dr. Brian Gladman, brg@gladman.uk.net, Worcester, UK. All rights reserved. TERMS Redistribution and use in source and binary forms, with or without modification, are permitted subject to the following conditions: <ol style="list-style-type: none">1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission. This software is provided "as is" with no express or implied warranties of correctness or fitness for purpose.
-----	--

Open SSL	<p>Copyright (c) 1998–2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:</p> <ol style="list-style-type: none"> 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).” 4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, contact openssl-core@openssl.org. 5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).” <p>THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS,” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.</p> <p>This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).</p>
MD5	<p>Copyright (C) 1990, RSA Data Security, Inc. All rights reserved. License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work.</p> <p>RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind.</p> <p>These notices must be retained in any copies of any part of this documentation and/or software.</p>

PPP	<p>Copyright (c) 1989 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.</p>
Zlib	<p>zlib.h. Interface of the zlib general purpose compression library version 1.1.4, March 11th, 2002. Copyright (C) 1995–2002 Jean-loup Gailly and Mark Adler. This software is provided "as is," without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:</p> <ol style="list-style-type: none"> 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. <p>Jean-loup Gailly: jloup@gzip.org; Mark Adler: madler@alumni.caltech.edu. The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files ftp://ds.internic.net/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format), and rfc1952.txt (gzip format).</p>

Product and Publication Details

Model Number:	STM
Publication Date:	September 2009
Product Family:	STM
Product Name:	ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10519-01
Publication Version Number	1.0

Contents

About This Manual

Conventions, Formats, and Scope	xiii
How to Print This Manual	xiv
Revision History	xiv

Chapter 1

Introduction

What Is the ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600?	1-1
What Can You Do with an STM?	1-2
Key Features and Capabilities	1-3
Stream Scanning for Content Filtering	1-4
Autosensing Ethernet Connections with Auto Uplink	1-4
Easy Installation and Management	1-5
Maintenance and Support	1-5
STM Model Comparison	1-5
Service Registration Card with License Keys	1-6
Package Contents	1-7
Hardware Features	1-7
Front Panel Ports and LEDs	1-8
Rear Panel Features	1-14
Bottom Panel With Product Label	1-15
Choosing a Location for the STM	1-17
Using the Rack-Mounting Kit	1-18

Chapter 2

Using the Setup Wizard to Provision the STM in Your Network

Choosing a Deployment Scenario	2-1
Gateway Deployment	2-1
Server Group	2-2
Segmented LAN Deployment	2-3

Understanding the Steps for Initial Connection	2-4
Qualified Web Browsers	2-5
Logging In to the STM	2-5
Understanding the Web Management Interface Menu Layout	2-8
Using the Setup Wizard to Perform the Initial Configuration	2-10
Setup Wizard Step 1 of 10: Introduction	2-10
Setup Wizard Step 2 of 11: Networking Settings	2-11
Setup Wizard Step 3 of 11: Time Zone	2-12
Setup Wizard Step 4 of 11: Email Security	2-14
Setup Wizard Step 5 of 11: Web Security	2-17
Setup Wizard Step 6 of 11: Email Notification Server Settings	2-19
Setup Wizard Step 7 of 11: Update Settings	2-21
Setup Wizard Step 8 of 11: HTTP Proxy Settings	2-23
Setup Wizard Step 9 of 11: Web Categories	2-24
Setup Wizard Step 10 of 11: Configuration Summary	2-26
Setup Wizard Step 11 of 11: Restarting the System	2-27
Verifying Proper Installation	2-27
Testing Connectivity	2-27
Testing HTTP Scanning	2-27
Registering the STM with NETGEAR	2-28
What to Do Next	2-30

Chapter 3

Performing Network and System Management

Configuring Network Settings	3-1
Configuring Session Limits and Timeouts	3-5
Configuring the HTTP Proxy Settings	3-7
About Users with Administrative and Guest Privileges	3-9
Changing Administrative Passwords and Timeouts	3-9
Configuring Remote Management Access	3-11
Using an SNMP Manager	3-13
Supported MIB Browsers	3-15
Managing the Configuration File	3-16
Backup Settings	3-16
Restore Settings	3-17
Reverting to Factory Default Settings	3-18

Updating the Software	3-19
Scheduling Updates	3-19
Performing a Manual Update	3-21
Critical Updates That Require a Restart	3-22
Configuring Date and Time Service	3-23
Managing Digital Certificates	3-25
Managing the Certificate for HTTPS Scans	3-26
Managing Untrusted Certificates	3-29
Managing the Quarantine Settings	3-30
Performance Management	3-31

Chapter 4

Content Filtering and Optimizing Scans

About Content Filtering and Scans	4-1
Default E-mail and Web Scan Settings	4-2
Configuring E-mail Protection	4-4
Customizing E-mail Protocol Scan Settings	4-4
Customizing E-mail Anti-Virus Settings	4-5
E-mail Content Filtering	4-11
Protecting Against E-mail Spam	4-14
Configuring Web and Services Protection	4-22
Customizing Web Protocol Scan Settings	4-22
Configuring Web Malware Scans	4-24
Configuring Web Content Filtering	4-26
Configuring Web URL Filtering	4-32
HTTPS Scan Settings	4-36
Specifying Trusted Hosts	4-39
Configuring FTP Scans	4-41
Configuring Application Control	4-44
Setting Scanning Exclusions and Web Access Exceptions	4-46
Setting Scanning Exclusions	4-47
Setting Web Access Exception Rules	4-48

Chapter 5

Managing Users, Groups, and Authentication

About Users, Groups, and Domains	5-1
Configuring Groups	5-2

- Creating and Deleting Groups by Name5-3
- Editing Groups by Name5-4
- Creating and Deleting Groups by IP Address and Subnet5-5
- Configuring User Accounts5-6
 - Creating and Deleting User Accounts5-6
 - Editing User Accounts5-8
- Configuring Authentication5-9
 - Understanding Active Directories and LDAP Configurations5-12
 - Creating and Deleting LDAP and Active Directory Domains5-16
 - Editing LDAP and Active Directory Domains5-19
 - Creating and Deleting RADIUS Domains5-19
 - Editing RADIUS Domains and Configuring VLANs5-22
- Global User Settings5-24
- Viewing and Logging Out Active Users5-25

Chapter 6

Monitoring System Access and Performance

- Configuring Logging, Alerts, and Event Notifications6-1
 - Configuring the E-mail Notification Server6-2
 - Configuring and Activating System, E-mail, and Syslog Logs6-3
 - Configuring Alerts6-8
- Monitoring Real-Time Traffic, Security, Statistics, and Web Usage6-11
 - Understanding the Information on the Dashboard Screen6-11
 - Monitoring Web Usage6-18
- Viewing System Status6-19
- Querying Logs and Generating Reports6-22
 - Querying the Logs6-22
 - Scheduling and Generating Reports6-28
- Viewing and Managing the Quarantine Files6-33
- Using Diagnostics Utilities6-40
 - Using the Network Diagnostic Tools6-41
 - Using the Realtime Traffic Diagnostics Tool6-42
 - Gathering Important Log Information and Generating a Network Statistics Report6-43
 - Restarting and Shutting Down the STM6-44

Chapter 7

Troubleshooting and Using Online Support

Basic Functioning	7-2
Power LED Not On	7-2
Test LED or Status LED Never Turns Off	7-2
LAN or WAN Port LEDs Not On	7-3
Troubleshooting the Web Management Interface	7-3
When You Enter a URL or IP Address a Time-out Error Occurs	7-4
Troubleshooting a TCP/IP Network Using a Ping Utility	7-5
Testing the LAN Path to Your STM	7-5
Testing the Path from Your PC to a Remote Device	7-6
Restoring the Default Configuration and Password	7-6
Problems with Date and Time	7-7
Using Online Support	7-8
Enabling Remote Troubleshooting	7-8
Installing Hot Fixes	7-9
Sending Suspicious Files to NETGEAR for Analysis	7-10
Accessing the Knowledge Base and Documentation	7-11

Appendix A

Default Settings and Technical Specifications

Appendix B

Related Documents

Index

About This Manual

The NETGEAR® ProSecure™ Web/Email Security Threat Management Appliance STM Reference Manual describes how to configure and troubleshoot a ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600. The information in this manual is intended for readers with intermediate computer and networking skills.

Conventions, Formats, and Scope


The conventions, formats, and scope of this manual are described in the following paragraphs:


- **Typographical conventions.** This manual uses the following typographical conventions:


<i>Italic</i>	Emphasis, books, CDs
Bold	User input, IP addresses, GUI screen text
Fixed	Command prompt, CLI text, code
<i>italic</i>	URL links

- **Formats.** This manual uses the following formats to highlight special messages:

	Note: This format is used to highlight information of importance or special interest.
---	--

	Tip: This format is used to highlight a procedure that will save time or resources.
---	--


	Warning: Ignoring this type of note might result in a malfunction or damage to the equipment.
---	--


	Danger: This is a safety warning. Failure to take heed of this notice might result in personal injury or death.
---	--

- **Scope.** This manual is written for the STM according to these specifications:

Product	ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600
Manual Publication Date	September 2009


For more information about network, Internet, firewall, and VPN technologies, click the links to the NETGEAR website in [Appendix B, “Related Documents.”](#)

	Note: Product updates are available on the NETGEAR website at http://prosecure.netgear.com or http://kb.netgear.com/app/home .
---	---

	Note: Go to http://prosecure.netgear.com/community/forum.php for information about the ProSecure™ forum and to become part of the ProSecure™ community.
---	---

How to Print This Manual

To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at <http://www.adobe.com>.

	Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.
---	---

Revision History

Manual Part Number	Manual Version Number	Publication Date	Description
202-10519-01	1.0	September 2009	Initial publication of this reference manual.

Chapter 1

Introduction

This chapter provides an overview of the features and capabilities of the ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600. It also identifies the physical features of the appliances and the contents of the product packages.

This chapter contains the following sections:

- [“What Is the ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600?”](#) on this page.
- [“What Can You Do with an STM?”](#) on page 1-2.
- [“Key Features and Capabilities”](#) on page 1-3.
- [“Service Registration Card with License Keys”](#) on page 1-6.
- [“Rear Panel Features”](#) on page 1-14.
- [“Bottom Panel With Product Label”](#) on page 1-15.
- [“Choosing a Location for the STM”](#) on page 1-17.

What Is the ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600?

The ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600, hereafter referred to as the STM, is an appliance-based, Web and e-mail security solution that protects the network perimeter against Web-borne threats from spyware, viruses, e-mail, and blended threats. Ideally deployed at the gateway, it serves as the network’s first line of defense against all types of threats, and complements firewalls, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), dedicated Intranet security products, and endpoint anti-virus and anti-spyware software.

Powered by patent-pending Stream Scanning technology and backed by one of the most comprehensive malware databases in the industry, the STM can detect and stop all known spyware and viruses at the gateway, preventing them from reaching your desktops and servers, where cleanup would be much more difficult.

In addition to scanning HTTP, HTTPS, FTP, SMTP, POP3, and IMAP traffic, the STM protects networks against spam phishing attacks and unwanted Web use. The STM is a plug-and-play device that can be installed and configured within minutes.

What Can You Do with an STM?

The STM combines robust protection against malware threats with ease of use and advanced reporting and notification features to help you deploy and manage the device with minimal effort.

Here are some of the things that you can do with the STM:

- **Protect the network instantly.** The STM is a plug-and-play security solution that can be instantly added to networks without requiring network reconfiguration.
- **Scan network traffic for malware.** Using the patent-pending Stream Scanning technology, you can configure the STM to scan HTTP, HTTPS, FTP, SMTP, POP3, and IMAP protocols. Unlike traditional batch-based scan engines that need to cache the entire file before they can scan, this scan engine checks traffic as it enters the network, ensuring unimpeded network performance.
- **Set access policies for individual users or groups.** You can configure Web and e-mail access access policies for individual users and groups based on the STM's local database, on group IP address, on LDAP domain, group, or user, or on RADIUS VLAN.
- **Receive real-time alerts and generate comprehensive reports.** You can configure the STM to send alerts when a malware attack or outbreak is detected on the network. Real-time alerts can be sent by e-mail, allowing you to monitor malware events wherever you are.

By configuring the STM to send malware alerts, you can isolate and clean the infected computer before the malware incident can develop into a full-blown outbreak. The STM also provides comprehensive reports that you can use to analyze network and malware trends.

- **Manage through SNMP support.** You can enable and configure the STM's SNMP settings to receive SNMP traps through a supported MIB browser.
- **Allow automated component updates.** Downloading components regularly is the key to ensuring updated protection against new threats. The STM makes this administrative task easier by supporting automatic malware pattern, program, and engine updates.

Key Features and Capabilities

The STM provides the following key features and capabilities:

- Up to two pairs of 10/100/1000 Mbps Gigabit Ethernet WAN ports (see [“STM Model Comparison” on page 1-5](#)).
- Scalable support (see [“STM Model Comparison” on page 1-5](#)) for:
 - up to 600 concurrent users
 - up to 6000 concurrently scanned HTTP sessions
 - up to 239 MB/s HTTP throughput
 - up to 960,000 e-mails per hour SMTP throughput.
- Patent-pending Stream Scanning technology that enables scanning of real-time protocols such as HTTP.
- Comprehensive Web and e-mail inbound and outbound security, covering six major network protocols: HTTP, HTTPS, FTP, SMTP, POP3, and IMAP.
- URL content filtering with 64 categories.
- Malware database containing hundreds of thousands of signatures of spyware, viruses, and other malware threats.
- Very frequently updated malware signatures, hourly if required. The STM can automatically check for new malware signatures as frequently as every 15 minutes.
- Multiple anti-spam technologies to provide extensive protection against unwanted e-mails.
- Spam and malware quarantine for easy analysis.
- Web application control, including access control for instant messaging, media applications, peer-to-peer applications, and Web-based tools and toolbars.
- User management with LDAP, Active Directory, and RADIUS integration, allowing access policy configuration per user and per group.
- Easy, Web-based wizard setup for installation and management.
- SNMP-manageable.
- Dedicated management interface. (This feature is model dependent, see [“STM Model Comparison” on page 1-5](#)).
- Hardware bypass port to prevent network disruption in case failure. (This feature is model dependent, see [“STM Model Comparison” on page 1-5](#)).
- Front panel LEDs for easy monitoring of status and activity.
- Internal universal switching power supply.

Stream Scanning for Content Filtering

Stream Scanning is based on the simple observation that network traffic travels in streams. The STM scan engine starts receiving and analyzing traffic as the stream enters the network. As soon as a number of bytes are available, scanning starts. The scan engine continues to scan more bytes as they become available, while at the same time another thread starts to deliver the bytes that have been scanned.

This multithreaded approach, in which the receiving, scanning, and delivering processes occur concurrently, ensures that network performance remains unimpeded. The result is file scanning is up to five times faster than with traditional anti-virus solutions—a performance advantage that you will notice.

Stream Scanning also enables organizations to withstand massive spikes in traffic, as in the event of a malware outbreak. The scan engine has the following capabilities:

- **Real-time protection.** The patent-pending Stream Scanning technology enables scanning of previously undefended real-time protocols, such as HTTP. Network activities susceptible to latency (for example, Web browsing) are no longer brought to a standstill.
- **Comprehensive protection.** Provides both Web and e-mail security, covering six major network protocols: HTTP, HTTPS, FTP, SMTP, POP3, and IMAP. The STM uses enterprise-class scan engines employing both signature-based and Distributed Spam Analysis to stop both known and unknown threats. The malware database contains hundreds of thousands of signatures of spyware, viruses, and other malware.
- **Objectionable traffic protection.** The STM prevents objectionable content from reaching your computers. You can control access to the Internet content by screening for Web categories, Web addresses, and Web services. You can log and report attempts to access objectionable Internet sites.
- **Automatic signature updates.** Malware signatures are updated as frequently as every hour, and the STM can check automatically for new signatures as frequently as every 15 minutes.

Autosensing Ethernet Connections with Auto Uplink

With its internal 10/100/1000 ports, the STM can connect to either a 10 Mbps standard Ethernet network, a 100 Mbps Fast Ethernet network, or a 1000 Mbps Gigabit Ethernet network. The interfaces are autosensing and capable of full-duplex or half-duplex operation.

The STM incorporates Auto Uplink™ technology. Each Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a “normal” connection such as to a PC or an “uplink” connection such as to a switch or hub. That port then configures itself to the correct configuration. This feature eliminates the need to think about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection.

Easy Installation and Management

You can install, configure, and operate the STM within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management.** Browser-based configuration allows you to easily configure the STM from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- **SNMP.** The STM supports the Simple Network Management Protocol (SNMP) to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.
- **Diagnostic functions.** The STM incorporates built-in diagnostic functions such as a Ping utility, Trace-route utility, DNS lookup utility, and remote restart.
- **Remote management.** The STM allows you to log in to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.
- **Visual monitoring.** The STM's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers technical support seven days a week, 24 hours a day, according to the terms identified in the Warranty and Support information card provided with your product.

STM Model Comparison

Table 1-1 compares the three STM models to show the differences:

Table 1-1. Differences Between the STM Models

Feature	STM150	STM300	STM600
Performance and Sizing Guidelines			
Concurrent Users	up to 150	up to 300	up to 600
Web Scan Throughput	43 Mbps	148 Mbps	239 Mbps
Concurrent Scanned HTTP Connections	1500	3000	6000
SMTP Throughput (e-mails per hour)	139,000	420,000	960,000

Table 1-1. Differences Between the STM Models (continued)

Feature	STM150	STM300	STM600
Hardware			
Gigabit RJ-45 Ports	Total of 5 ports: • 1 uplink • 4 downlink	Total of 3 ports: • 1 pair of ports (1 uplink and 1 downlink) • 1 management	Total of 5 ports: • 2 pairs of ports ^a (2 uplink and 2 downlink) • 1 management
Gigabit RJ45 Port Pairs with Failure Bypass	0	1 pair of ports	2 pairs of ports
Dedicated Management VLAN RJ45 Ports	0	1	1

a. The STM600 provides two pairs of ports, allowing for support of two separate networks or subnets with strict traffic separation.

Service Registration Card with License Keys

Be sure to store the license key card that came with your STM in a secure location. You do need these keys to activate your product during the initial setup.



Figure 1-1



Note: When you reset the STM to the original factory default settings after you have entered the license keys to activate the STM (see [“Registering the STM with NETGEAR” on page 2-28](#)), the license keys are erased. The license keys and the different types of licenses that are available for the STM are no longer displayed on the Registration screen. However, after you have reconfigured the STM to connect to the Internet and to the NETGEAR registration server, the STM retrieves and restores all registration information based on its MAC address and hardware serial number. You do not need to re-enter the license keys and reactivate the STM.

Package Contents

The STM product package contains the following items:

- ProSecure Web/Email Security Threat Management Appliance STM150, STM300, or STM600
- One AC power cable
- Rubber feet (4) with adhesive backing
- One rack-mount kit
- Straight through Category 5 Ethernet Cable
- *ProSecure™ Web/Email Security Threat Management Appliance STM150, STM300, or STM600 Installation Guide*
- Depending on the model purchased, Service Registration Card with License Key(s)
- Warranty and Support Information Card

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

Hardware Features

The front panel ports and LEDs, rear panel ports, and bottom label of the STM models are described in this section.

Front Panel Ports and LEDs

The front panels of the three STM models provide different components.

STM150 Front Panel

Figure 1-2 shows the front panel ports and status light-emitting diodes (LEDs) of the STM150.

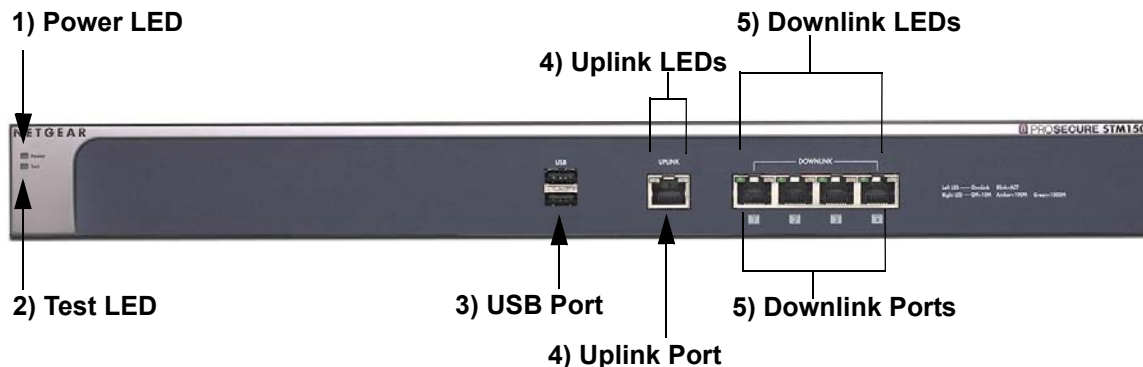


Figure 1-2

From left to right, the STM150's front panel shows the following ports and LEDs:

1. Power LED.
2. Test LED.
3. One non-functioning USB port: this port is included for future management enhancements. The port is currently not operable on any STM model.
4. One uplink (WAN) Gigabit Ethernet port with an RJ-45 connector, left LED, and right LED.
5. Four downlink (LAN) Gigabit Ethernet ports with RJ-45 connectors, left LEDs, and right LEDs.



Note: All Gigabit Ethernet ports provide switched N-way, automatic speed-negotiating, auto MDI/MDIX technology.

The function of each STM150 LED is described in the following table:

Table 1-2. LED Descriptions for the STM150

Object	Activity	Description
Power	On (Green)	Power is supplied to the STM.
	Off	Power is not supplied to the STM.
Test	On (Amber) during startup.	The STM is initializing. After approximately 2 minutes, when the STM has completed its initialization, the Test LED turns off. If the Test LED remains on, the initialization has failed.
	Off	The system has completed its initialization successfully. The Test LED should be off during normal operation.
	Blinking (Amber)	The STM is shutting down.
		Software is being updated.
A hot fix is being installed.		
One of the three licenses has expired. To stop the Test LED from blinking, renew the license, or click the Stop LED Blinking button on the System Status screen (see " Viewing System Status " on page 6-19).		
Uplink (WAN) Port		
Left LED	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the STM.
	On (Green)	The WAN port has a valid connection with a device that provides an Internet connection.
	Blink (Green)	Data is being transmitted or received by the WAN port.
Right LED	Off	The WAN port is operating at 10 Mbps.
	On (Amber)	The WAN port is operating at 100 Mbps.
	On (Green)	The WAN port is operating at 1000 Mbps.
Downlink (LAN) Ports		
Left LED	Off	The LAN port has no link.
	On (Green)	The LAN port has detected a link with a connected Ethernet device.
	Blink (Green)	Data is being transmitted or received by the LAN port.
Right LED	Off	The LAN port is operating at 10 Mbps.
	On (Amber)	The LAN port is operating at 100 Mbps.
	On (Green)	The LAN port is operating at 1000 Mbps.

Front Panel STM300

Figure 1-3 shows the front panel ports and LEDs of the STM300.

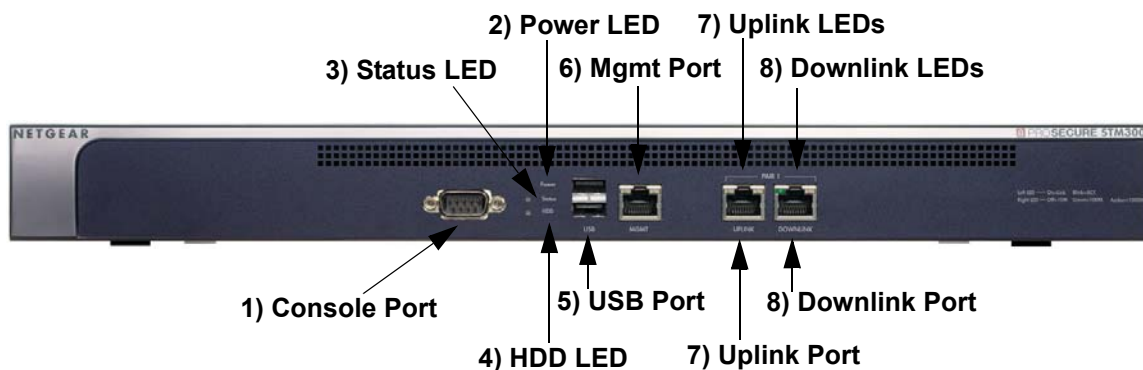


Figure 1-3

From left to right, the STM300's front panel shows the following ports and LEDs:

1. Console port. Port for connecting to an optional console terminal. The ports has a DB9 male connector. The default baud rate is 9600 K. The pinouts are: (2) Tx, (3) Rx, (5) and (7) Gnd.
2. Power LED.
3. Status LED.
4. Hard drive (HDD) LED.
5. One non-functioning USB port: this port is included for future management enhancements. The port is currently not operable on any STM model.
6. Dedicated management (Mgmt) Gigabit Ethernet port with an RJ-45 connector.
7. One uplink (WAN) Gigabit Ethernet port with an RJ-45 connector, left LED, and right LED.
8. One downlink (LAN) Gigabit Ethernet port with RJ-45 connectors, left LEDs, and right LED.



Note: All Gigabit Ethernet ports provide switched N-way, automatic speed-negotiating, auto MDI/MDIX technology.

The function of each STM300 LED is described in the following table:

Table 1-3. LED Descriptions for the STM300

Object	Activity	Description
Power	On (Green)	Power is supplied to the STM.
	Off	Power is not supplied to the STM.
Status	On (Amber) during startup.	The STM is initializing. After approximately 2 minutes, when the STM has completed its initialization, the Status LED turns off. If the Status LED remains on, the initialization has failed.
	Off	The system has completed its initialization successfully. The Status LED should be off during normal operation.
	Blinking (Amber)	The STM is shutting down.
		Software is being updated.
A hot fix is being installed.		
		One of the three licenses has expired. To stop the Status LED from blinking, renew the license, or click the Stop LED Blinking button on the System Status screen (see "Viewing System Status" on page 6-19).
HDD	On (Green)	Information is being written to the hard drive.
	Off	No hard drive activity.
Uplink (WAN) Port		
Left LED	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the STM.
	On (Green)	The WAN port has a valid connection with a device that provides an Internet connection.
	Blink (Green)	Data is being transmitted or received by the WAN port.
Right LED	Off	The WAN port is operating at 10 Mbps.
	On (Green)	The WAN port is operating at 100 Mbps.
	On (Amber)	The WAN port is operating at 1000 Mbps.
Downlink (LAN) Ports		
Left LED	Off	The LAN port has no link.
	On (Green)	The LAN port has detected a link with a connected Ethernet device.
	Blink (Green)	Data is being transmitted or received by the LAN port.
Right LED	Off	The LAN port is operating at 10 Mbps.
	On (Green)	The LAN port is operating at 100 Mbps.
	On (Amber)	The LAN port is operating at 1000 Mbps.

Front Panel STM600

Figure 1-4 shows the front panel ports and LEDs of the STM600.

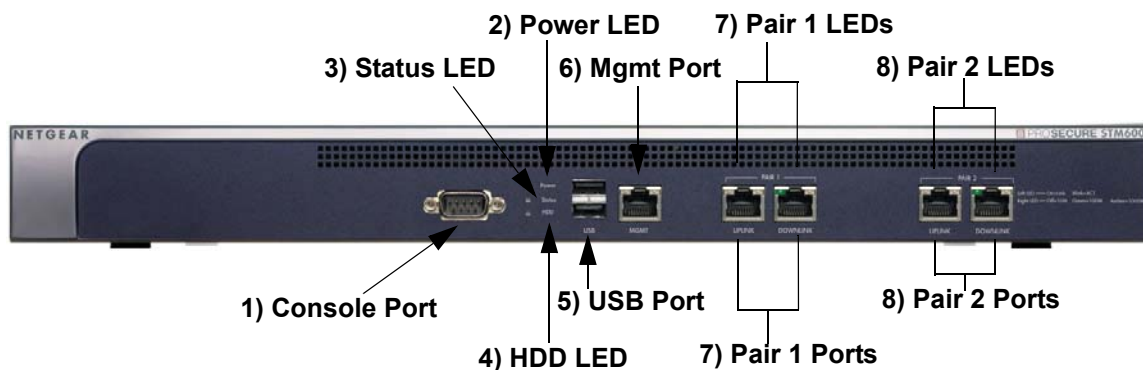


Figure 1-4

From left to right, the STM600's front panel shows the following ports and LEDs:

1. Console port. Port for connecting to an optional console terminal. The ports has a DB9 male connector. The default baud rate is 9600 K. The pinouts are: (2) Tx, (3) Rx, (5) and (7) Gnd.
2. Power LED.
3. Status LED.
4. Hard drive (HDD) LED.
5. One non-functioning USB port: this port is included for future management enhancements. The port is currently not operable on any STM model.
6. Dedicated management (Mgmt) Gigabit Ethernet port with an RJ-45 connector.
7. Pair 1 uplink (WAN) and downlink (LAN) Gigabit Ethernet ports with RJ-45 connectors, left LEDs, and right LEDs.
8. Pair 2 uplink (WAN) and downlink (LAN) Gigabit Ethernet ports with RJ-45 connectors, left LEDs, and right LEDs.



Note: All Gigabit Ethernet ports provide switched N-way, automatic speed-negotiating, auto MDI/MDIX technology.

The function of each STM600 LED is described in the following table:

Table 1-4. LED Descriptions for the STM600

Object	Activity	Description
Power	On (Green)	Power is supplied to the STM.
	Off	Power is not supplied to the STM.
Status	On (Amber) during startup.	The STM is initializing. After approximately 2 minutes, when the STM has completed its initialization, the Status LED turns off. If the Status LED remains on, the initialization has failed.
	Off	The system has completed its initialization successfully. The Status LED should be off during normal operation.
	Blinking (Amber)	The STM is shutting down.
		Software is being updated.
A hot fix is being installed.		
		One of the three licenses has expired. To stop the Status LED from blinking, renew the license, or click the Stop LED Blinking button on the System Status screen (see "Viewing System Status" on page 6-19).
HDD	On (Green)	Information is being written to the hard drive.
	Off	No hard drive activity.
Uplink (WAN) Port		
Left LED	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the STM.
	On (Green)	The WAN port has a valid connection with a device that provides an Internet connection.
	Blink (Green)	Data is being transmitted or received by the WAN port.
Right LED	Off	The WAN port is operating at 10 Mbps.
	On (Green)	The WAN port is operating at 100 Mbps.
	On (Amber)	The WAN port is operating at 1000 Mbps.
Downlink (LAN) Ports		
Left LED	Off	The LAN port has no link.
	On (Green)	The LAN port has detected a link with a connected Ethernet device.
	Blink (Green)	Data is being transmitted or received by the LAN port.
Right LED	Off	The LAN port is operating at 10 Mbps.
	On (Green)	The LAN port is operating at 100 Mbps.
	On (Amber)	The LAN port is operating at 1000 Mbps.

Rear Panel Features

The rear panel of the STM150 differs from the rear panels of the STM300 and STM600.

Rear Panel STM150

Figure 1-5 shows the rear panel components of the STM150.

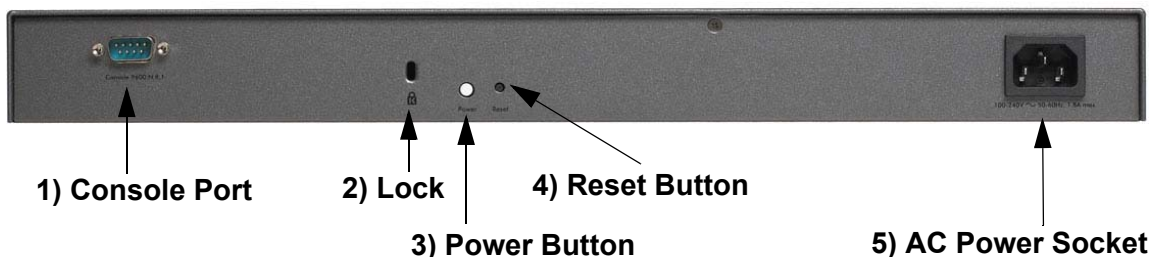


Figure 1-5

From left to right, the STM150's rear panel components are:

1. Console port. Port for connecting to an optional console terminal. The ports has a DB9 male connector. The default baud rate is 9600 K. The pinouts are: (2) Tx, (3) Rx, (5) and (7) Gnd.
2. Kensington lock. Attach an optional Kensington lock to prevent unauthorized removal of the STM150.
3. Power Button. Press to restart the STM150. Restarting does not reset the STM150 to its factory defaults.
4. Reset Button. Using a sharp object, press and hold this button for about 10 seconds until the front panel Test light flashes and the STM150 returns to factory default settings.



Note: If you reset the STM150, all configuration settings are lost and the default passwords are restored.

5. AC power socket. Attach the power cord to this socket.

Rear Panel STM300 and STM600

The rear panels of the STM300 and STM600 are identical.

Figure 1-6 shows the rear panel components of the STM300 and STM600.



Figure 1-6

From left to right, the STM300's and STM600's rear panel components (excluding the four fan air outlets) are:

1. Power switch. Switch to turn the STM300 or STM600 on or off. Restarting does not reset the STM300 or STM600 to its factory defaults.



Note: The STM300 and STM600 do not provide a Reset button. To reset the STM300 or STM600 to factory default setting using the Web Management Interface, see [“Reverting to Factory Default Settings” on page 3-18](#).

2. AC power socket. Attach the power cord to this socket.

Bottom Panel With Product Label

The product label on the bottom of the STM's enclosure displays the STM's default IP address, default user name, and default password, as well as regulatory compliance, input power, and other information.

STM150 Product Label



Figure 1-7

STM300 Product Label



Figure 1-8

STM600 Product Label



Figure 1-9

Choosing a Location for the STM

The STM is suitable for use in an office environment where it can be free-standing (on its runner feet) or mounted into a standard 19-inch equipment rack. Alternatively, you can rack-mount the STM in a wiring closet or equipment room. A mounting kit, containing two mounting brackets and four screws, is provided in the STM package.

Consider the following when deciding where to position the STM:

- The unit is accessible and cables can be connected easily.
- Cabling is away from sources of electrical noise. These include lift shafts, microwave ovens, and air-conditioning units.
- Water or moisture cannot enter the case of the unit.
- Airflow around the unit and through the vents in the side of the case is not restricted. Provide a minimum of 25 mm or 1 inch clearance.
- The air is as free of dust as possible.

- Temperature operating limits are not likely to be exceeded. Install the unit in a clean, air-conditioned environment. For information about the recommended operating temperatures for the STM, see [Appendix A, “Default Settings and Technical Specifications.”](#)

Using the Rack-Mounting Kit

Use the mounting kit for the STM to install the appliance in a rack. (A mounting kit is provided in the product package for the STM). The mounting brackets that are supplied with the STM are usually installed before the unit is shipped out. If the brackets are not yet installed, attach them using the supplied hardware.

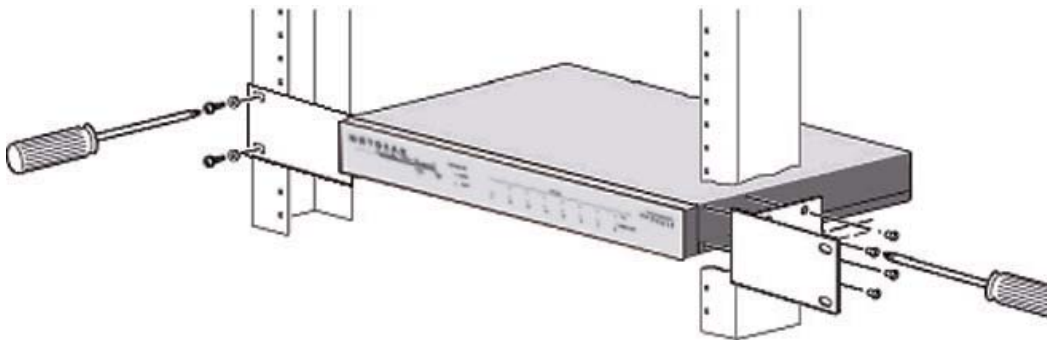


Figure 1-10

Before mounting the STM in a rack, verify that:

- You have the correct screws (supplied with the installation kit).
- The rack onto which you will mount the STM is suitably located.

Chapter 2

Using the Setup Wizard to Provision the STM in Your Network

This chapter describes provisioning the STM in your network. This chapter contains the following sections:

- [“Choosing a Deployment Scenario”](#) on this page.
- [“Understanding the Steps for Initial Connection”](#) on page 2-4.
- [“Registering the STM with NETGEAR”](#) on page 2-28.
- [“Verifying Proper Installation”](#) on page 2-27.
- [“Verifying Proper Installation”](#) on page 2-27.
- [“What to Do Next”](#) on page 2-30.

Choosing a Deployment Scenario

The STM is an inline transparent bridge appliance that can easily be deployed to any point on the network without requiring network reconfiguration or additional hardware.

The following are the most common deployment scenarios for the STM. Depending on your network environment and the areas that you want to protect, you can choose one or a combination of the deployment scenarios that are described in the following sections:

- [“Gateway Deployment”](#) on page 2-1.
- [“Server Group”](#) on page 2-2.
- [“Segmented LAN Deployment”](#) on page 2-3.

Gateway Deployment

In a typical gateway deployment scenario, a single STM appliance is installed at the gateway—between the firewall and the LAN core switch—to protect the network against all malware threats entering and leaving the gateway. Installing the STM behind the firewall protects it from denial of service (DoS) attacks. [Figure 2-1 on page 2-2](#) shows a typical gateway deployment scenario.

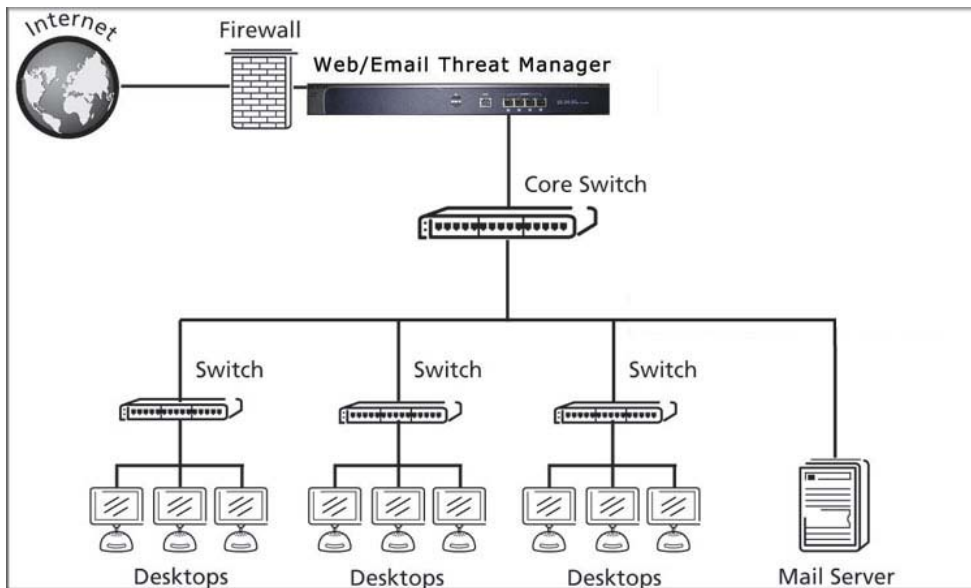


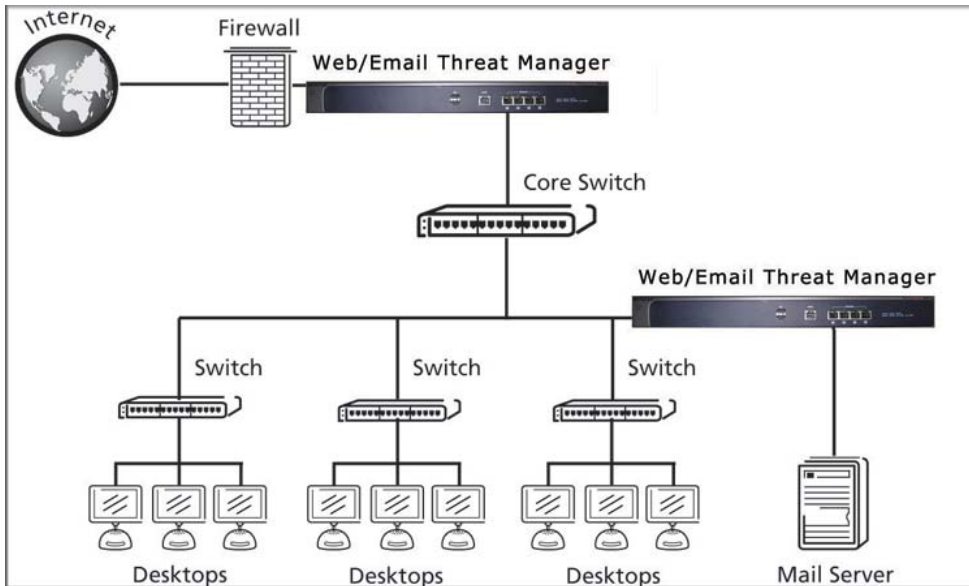
Figure 2-1

Server Group

In a server group deployment, one STM appliance is installed at the gateway and another in front of the server group. This type of deployment helps split the network load and provides the e-mail server with dedicated protection against malware threats, including e-mail-borne viruses and spam. [Figure 2-2 on page 2-3](#) shows a typical server group deployment scenario.



Note: This configuration helps protect the e-mail server from threats from internal as well as external clients.

**Figure 2-2**

Segmented LAN Deployment

In a segmented LAN deployment, one STM appliance is installed in front of each network segment. This type of deployment helps split the network load and protects network segments from malware threats coming in through the gateway or originating from other segments. [Figure 2-3 on page 2-4](#) shows a typical segmented LAN deployment scenario.



Note: In a segmented LAN deployment, VLAN traffic can pass through the STM and can be scanned by the STM.

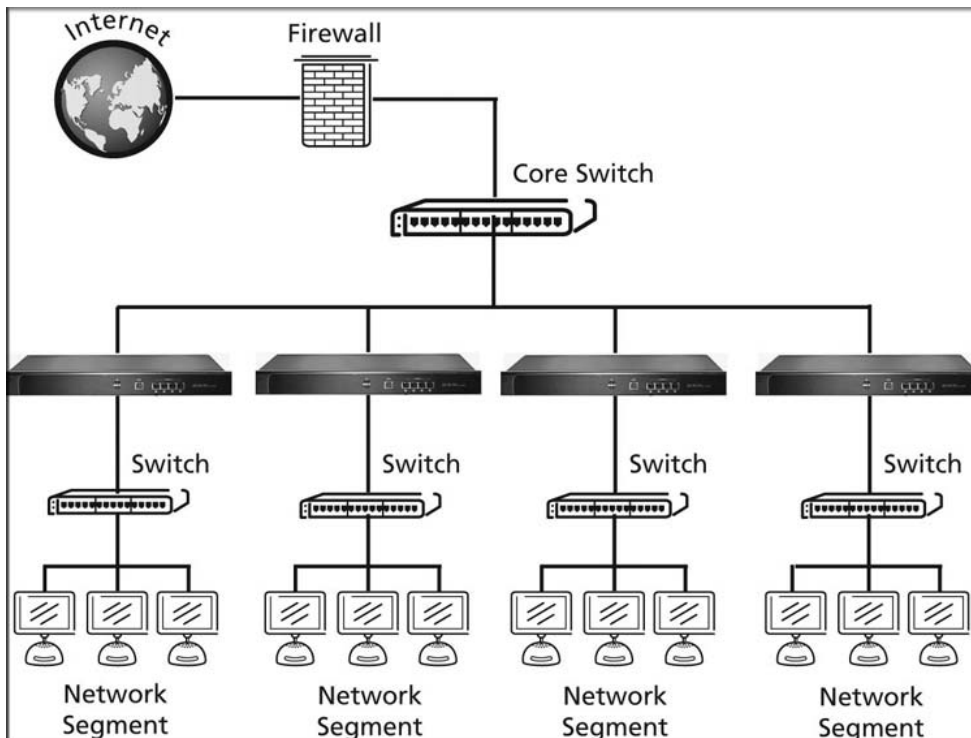


Figure 2-3

Understanding the Steps for Initial Connection

Generally, five steps are required to complete the basic and security configuration of your STM:

1. **Connect the STM physically to your network.** Connect the cables and restart your network according to the instructions in the installation guide. See the *ProSecure™ Web/Email Security Threat Management Appliance STM150, STM300, or STM600 Installation Guide* for complete steps. A PDF of the *Installation Guide* is on the NETGEAR ProSecure™ website at <http://prosecure.netgear.com> or <http://kb.netgear.com/app/home>.
2. **Log in to the STM.** After logging in, you are ready to set up and configure your STM. See “[Logging In to the STM](#)” on page 2-5.
3. **Use the Setup Wizard to configure basic connections and security.** During this phase, you connect the STM to your network. See “[Verifying Proper Installation](#)” on page 2-27.

4. **Verify the installation.** See “[Verifying Proper Installation](#)” on page 2-27.
5. **Register the STM.** “[Registering the STM with NETGEAR](#)” on page 2-28.

Each of these tasks is described separately in this chapter.

Qualified Web Browsers

To configure the STM, you must use a Web browser such as Microsoft Internet Explorer 5.1 or higher, Mozilla Firefox 1.x or higher, or Apple Safari 1.2 or higher with JavaScript, cookies, and you must have SSL enabled.

Although these web browsers are qualified for use with the STM’s Web Management Interface, SSL VPN users should choose a browser that supports JavaScript, Java, cookies, SSL, and ActiveX to take advantage of the full suite of applications. Note that Java is only required for the SSL VPN portal, not for the Web Management Interface.

Logging In to the STM


To connect to the STM, your computer needs to be configured to obtain an IP address automatically from the STM via DHCP. For instructions on how to configure your computer for DHCP, see the document that you can access from “[Preparing Your Network](#)” in [Appendix B](#).

To connect and log in to the STM:

1. Start any of the qualified browsers, as explained in “[Qualified Web Browsers](#)” on this page.
2. Enter **https://192.168.1.201** in the address field.



Figure 2-4

	<p>Note: The STM factory default IP address is 192.168.1.201. If you change the IP address, you must use the IP address that you assigned to the STM to log in to the STM.</p>
---	---

The NETGEAR Configuration Manager Login screen displays in the browser (see [Figure 2-4](#), which shows the STM600).

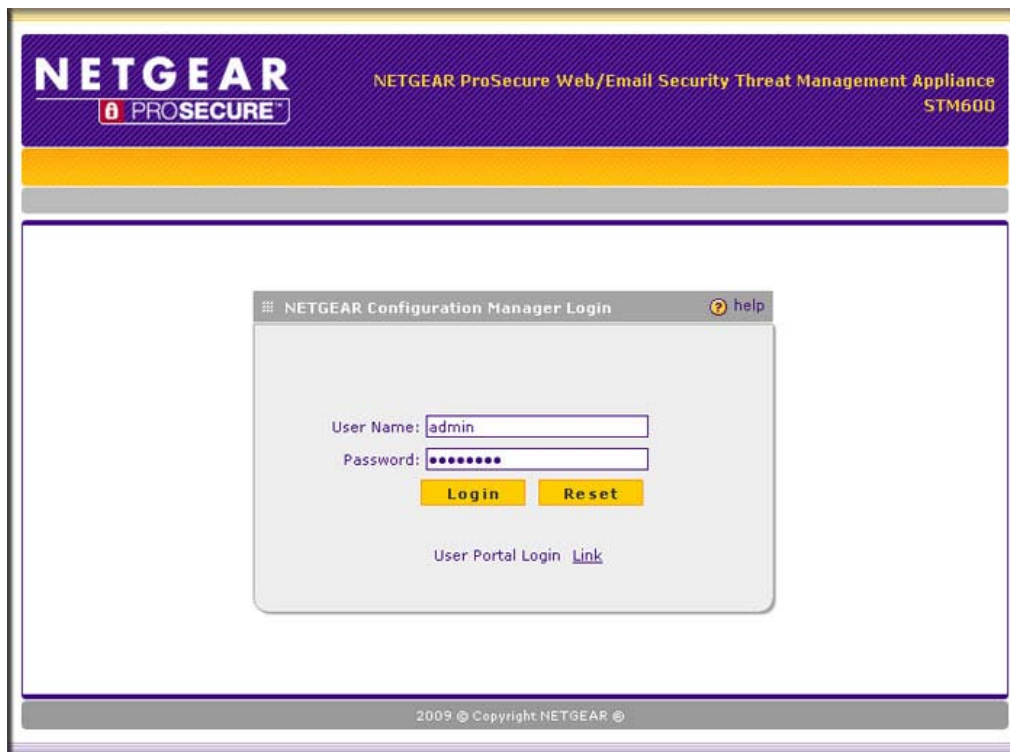



Figure 2-5


3. In the User field, type **admin**. Use lower case letters.
4. In the Password field, type **password**. Here too, use lower case letters.




Note: The STM user name and password are not the same as any user name or password you might use to log in to your Internet connection.

 **Note:** The first time that you remotely connect to the STM with a browser via an SSL VPN connection, you might get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or higher, simply click Yes to accept the certificate. Other browsers provide you with similar options to accept and install the SSL certificate. If you connect to the STM through the User Portal login screen (see [Figure 5-7 on page 5-10](#)), you can import the STM's root certificate by clicking the hyperlink at the bottom of the screen.

5. Click **Login**. The Web Management Interface appears, displaying the Dashboard screen. ([Figure 2-2 on page 2-3](#) shows the top part of the screen. For information about this screen, see “[Understanding the Information on the Dashboard Screen](#)” on page 6-11.

 **Note:** After 5 minutes of inactivity (the default login time-out), you are automatically logged out.

 **Note:** During the initial setup, the Setup Wizard displays when you first log in; afterward the login takes you to the Dashboard screen.

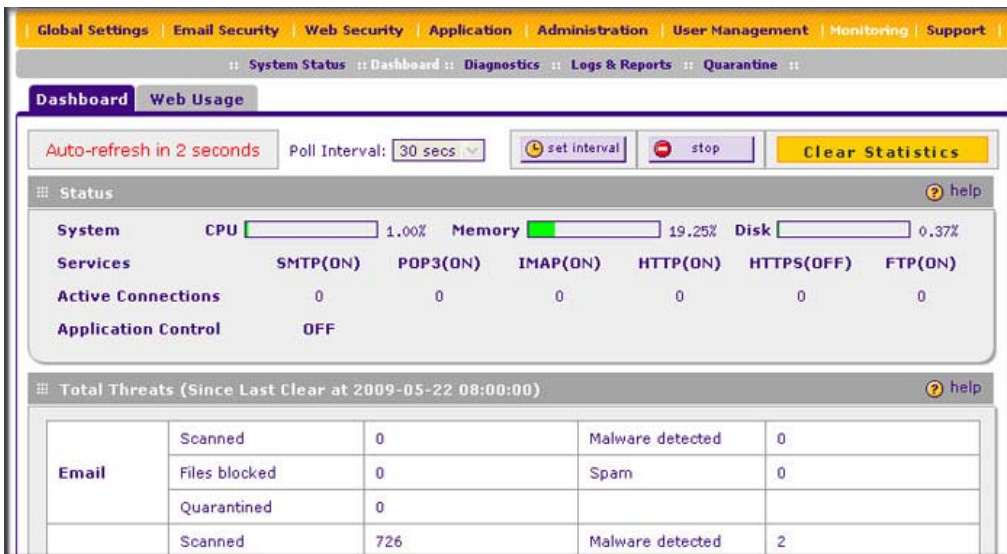


Figure 2-6

Understanding the Web Management Interface Menu Layout

Figure 2-7 shows the menu at the top of the STM600's Web Management Interface. The Web Management Interface layouts of the STM150 and STM300 are identical.



Figure 2-7

The Web Management Interface menu consists of the following components:

- **1st Level: Main navigation menu links.** The main navigation menu in the orange bar across the top of the Web Management Interface provide access to all the configuration functions of the STM, and remain constant. When you select a main navigation menu link, the letters are displayed in white against an orange background.
- **2nd Level: Configuration menu links.** The configuration menu links in the gray bar (immediately below the main navigation menu bar) change according to the main navigation menu link that you select. When you select a configuration menu link, the letters are displayed in white against a grey background.
- **3rd Level: Submenu tabs.** Each configuration menu item has one or more submenu tabs that are listed below the grey menu bar. When you select a submenu tab, the text is displayed in white against a blue background.

The bottom of each screen provides action buttons. The nature of the screen determines which action buttons are shown Figure 2-8 shows an example.



Figure 2-8

Any of the following action buttons might be displayed on screen (this list might not be complete):

- **Apply.** Save and apply the configuration.
- **Reset.** Reset the configuration to default values.
- **Test.** Test the configuration before you decide whether or not to save and apply the configuration.
- **Auto Detect.** Enable the STM to detect the configuration automatically and suggest values for the configuration.
- **Next.** Go to the next screen (for wizards).
- **Back.** Go to the previous screen (for wizards).
- **Search.** Perform a search operation.
- **Cancel.** Cancel the operation.
- **Send Now.** Send a file or report.

When a screen includes a table, table buttons are displayed to let you configure the table entries. The nature of the screen determines which table buttons are shown. [Figure 2-9](#) shows an example.

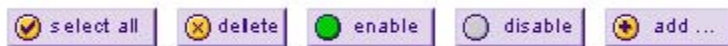



Figure 2-9

Any of the following table buttons might be displayed on screen:

- **select all.** Select all entries in the table.
- **delete.** Delete the selected entry or entries from the table.
- **enable.** Enable the selected entry or entries in the table.
- **disable.** Disable the selected entry or entries in the table.
- **add.** Add an entry to the table.
- **edit.** Edit the selected entry.

Almost all screens and sections of screens have an accompanying help screen. To open the help screen, click the question mark icon. ().

Using the Setup Wizard to Perform the Initial Configuration

The Setup Wizard facilitates the initial configuration of the STM by taking you through 11 screens, the last of which allows you to save the configuration.

To start the Setup Wizard:

1. Select **Global Settings** > **Network Settings** from the main navigation menu. The Network Settings submenu tabs appear with the Network Settings screen in view.
2. From the Global Setting configuration menu, select **Setup Wizard**.

The following sections explain the 11 configuration screens of the Setup Wizard. On the 10th screen, you can save your configuration. The 11th screen is just an informational screen.

The tables in the following sections explain the buttons and fields of the Setup Wizard screens. Additional information about the settings in the Setup Wizard screens is provided in other chapters that explain manual configuration; each section below provides a specific link to a section in another chapters.

Setup Wizard Step 1 of 10: Introduction

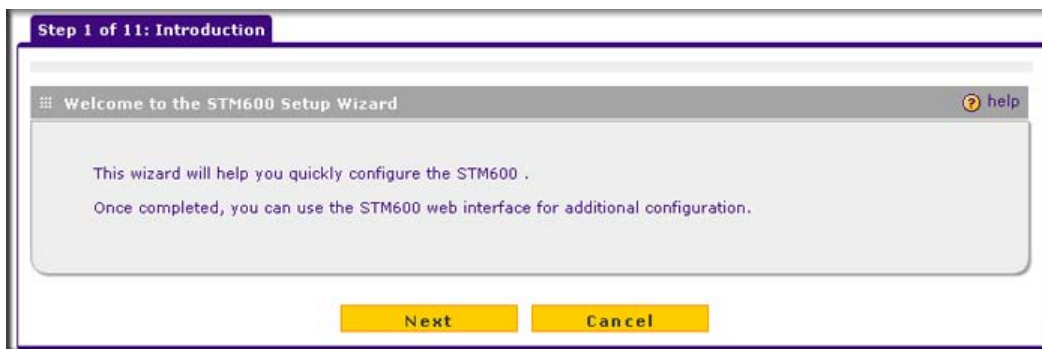


Figure 2-10

The first Setup Wizard screen is just an introductory screen. Click **Next** to go to the following screen.

Setup Wizard Step 2 of 11: Networking Settings

Step 2 of 11: Networking Setting

Management Interface Settings help

System Name:

IP Address:

Subnet Mask:

Gateway Address:

Primary DNS:

Secondary DNS: (optional)

MTU Settings help

Maximum Transmission Unit:

Back **Next** **Cancel**

Figure 2-11

Enter the settings as explained in [Table 2-1](#), then click **Next** to go the following screen.

	<p>Note: After you have completed the steps in the Setup Wizard, you can make changes to the network settings by selecting Global Settings > Network Settings. For more information about these network settings, see “Configuring Network Settings” on page 3-1.</p>
--	--

Table 2-1. Setup Wizard Step 2: Network Settings

Setting	Description (or Subfield and Description)
Management Interface Settings	
System Name	The name for the STM for purposes of identification and management. The default name is the name of your model (STM150, STM300, or STM600).
IP Address	Enter the IP address of the STM through which you will access the Web Management Interface. The factory default IP address is 192.168.1.201. Note: If you change the IP address of the STM while being connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again. For example, if you change the default IP address from 192.168.1.201 to 10.0.0.1, you must now enter https://10.0.0.1 in your browser to reconnect to the Web Management Interface.

Table 2-1. Setup Wizard Step 2: Network Settings (continued)

Setting	Description (or Subfield and Description)
Subnet Mask	Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask.
Gateway Address	Enter the IP address of the gateway through which the STM is accessed.
Primary DNS	Specify the IP address for the primary DNS server IP address.
Secondary DNS	As an option , specify the IP address for the secondary DNS server IP address.
MTU Settings	
Maximum Transmission Unit	The maximum transmission unit (MTU) is the largest physical packet size that a network can transmit. Packets that are larger than the MTU value are divided into smaller packets before they are sent, an action that prolongs the transmission process. For most Ethernet networks the MTU value is 1500 Bytes, which is the default setting. Note: NETGEAR recommends synchronizing the STM's MTU setting with that of your network to prevent delays in transmission.

Setup Wizard Step 3 of 11: Time Zone

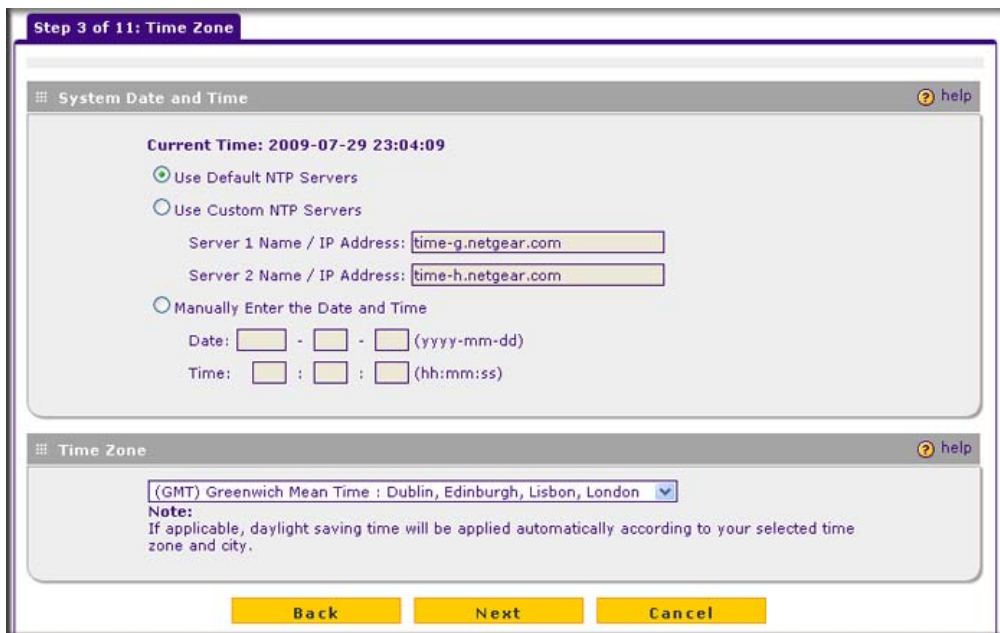


Figure 2-12

Enter the settings as explained in [Table 2-2](#), then click **Next** to go the following screen.


	<p>Note: After you have completed the steps in the Setup Wizard, you can make changes to the date and time by selecting Administration > System Date & Time. For more information about these settings, see “Configuring Date and Time Service” on page 3-23.</p>
---	--

Table 2-2. Setup Wizard Step 3: System Date and Time Settings

Setting	Description (or Subfield and Description)	
System Date and Time		
From the pull-down menu, select an NTP server, or select to enter the time manually.		
Use Default NTP Servers	The STM's real-time clock (RTC), which it uses for scheduling, is updated regularly by contacting a default Netgear NTP server on the Internet. This is the default setting.	
Use Custom NTP Servers	The STM's RTC is updated regularly by contacting one of the two NTP servers (primary and backup), both of which you must specify in the fields that become available with this menu selection. Note: If you select this option but leave either the Server 1 or Server 2 field blank, both fields are automatically set to the default Netgear NTP servers. Note: A list of public NTP servers is available at http://ntp.isc.org/bin/view/Servers/WebHome .	
	Server 1 Name / IP Address	Enter the IP address or host name the primary NTP server.
	Server 2 Name / IP Address	Enter the IP address or host name the secondary NTP server.
Manually Enter the Date and Time	Date	Enter the date in the yyyy-mm-dd (year-month-date) format.
	Time	Enter the time in the hh-mm-ss (hour-minutes-seconds) format.
Time Zone		
From the pull-down menu, select the local time zone in which the STM operates. The proper time zone is required in order for scheduling to work correctly. You do not need to configure daylight savings time, which is applied automatically when applicable. Greenwich Mean Time (GMT) is the default setting. Note: When you select a time zone that is not associated with a location such as “(GMT -08:00) GMT-8”, daylight savings time is automatically disabled. When you select a time zone that <i>is</i> associated with a location such as “(GMT -08:00) Pacific Time (US & Canada)”, daylight savings time is automatically enabled.		

Setup Wizard Step 4 of 11: Email Security

Step 4 of 11: Email Security

Services to Scan help

Enable	Service	Ports to Scan
<input checked="" type="checkbox"/>	SMTP	25
<input checked="" type="checkbox"/>	POP3	110
<input checked="" type="checkbox"/>	IMAP	143

Scan Action help

Service	Action
SMTP	Block infected email
POP3	Delete attachment
IMAP	Delete attachment


Scan Exceptions help

Skip if the file or message is larger than KB (Maximum: 51200 KB)

Back **Next** **Cancel**

Figure 2-13

Enter the settings as explained in [Table 2-3 on page 2-15](#), then click **Next** to go the following screen.

 **Note:** After you have completed the steps in the Setup Wizard, you can make changes to the e-mail security settings by selecting **Email Security > Policy** or **Email Security > Anti-Virus**. The Email Anti-Virus screen also lets you specify notification settings and e-mail alert settings. For more information about these settings, see [“Configuring E-mail Protection” on page 4-4](#).


 **Tip:** To enhance performance, you can disable scanning of any protocols that are seldom or never used. Be mindful of the difference between user- and server-generated traffic. For example, your mail server might not use IMAP, but some users might configure IMAP clients.

Table 2-3. Setup Wizard Step 4: Email Security Settings

Setting	Description (or Subfield and Description)	
Services to Scan		
SMTP	SMTP scanning is enabled by default on standard service port 25.	To disable any of these services, deselect the corresponding checkbox. You can change the standard service port or add another port in the corresponding Ports to Scan field.
POP3	POP3 scanning is enabled by default on standard service port 110.	
IMAP	IMAP scanning is enabled by default on standard service port 143.	
Scan Action		
SMTP	<p>From the SMTP pull-down menu, specify one of the following actions when an infected e-mail is detected:</p> <ul style="list-style-type: none"> • Quarantine attachment. The e-mail is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Delete attachment. The e-mail is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created. • Block infected email. This is the default setting. The e-mail is blocked, and a virus log entry or a spyware log entry is created. • Quarantine infected email. The e-mail is placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Log only. Only a virus log entry or a spyware log entry is created. The e-mail is not blocked and the attachment is not deleted. 	
POP3	<p>From the POP3 pull-down menu, specify one of the following actions when an infected e-mail is detected:</p> <ul style="list-style-type: none"> • Quarantine attachment. The e-mail is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Delete attachment. This is the default setting. The e-mail is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created. • Log only. Only a virus log entry or a spyware log entry is created. The e-mail is not blocked and the attachment is not deleted. 	

Table 2-3. Setup Wizard Step 4: Email Security Settings (continued)

Setting	Description (or Subfield and Description)
IMAP	<p>From the IMAP pull-down menu, specify one of the following actions when an infected e-mail is detected:</p> <ul style="list-style-type: none"> • Quarantine attachment. The e-mail is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Delete attachment. This is the default setting. The e-mail is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created. • Log only. Only a virus log entry or a spyware log entry is created. The e-mail is not blocked and the attachment is not deleted.
Scan Exceptions	
<p>From the pull-down menu, specify one of the following actions when an e-mail attachment exceeds the size that you specify in the file size field:</p> <ul style="list-style-type: none"> • Skip. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • Block. The file is blocked and does not reach the end user. <p>The default and maximum file sizes are:</p> <ul style="list-style-type: none"> • For the STM600 and STM300, the default setting is to block any attachment larger than 10240 KB. The maximum file size that you can specify is 51200 KB. • For the STM150, the default setting is to block any attachment larger than 8192 KB. The maximum file size that you can specify is 25600 KB. <p>Note: Setting the maximum file size to a high value might affect the STM's performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats.</p>	

Setup Wizard Step 5 of 11: Web Security

Step 5 of 11: Web Security

Services to Scan help

Enable	Service	Ports to Scan
<input checked="" type="checkbox"/>	HTTP	80
<input type="checkbox"/>	HTTPS	443
<input checked="" type="checkbox"/>	FTP	21

Scan Action help

Service	Action	Streaming
HTTP	Delete file	<input checked="" type="checkbox"/>
HTTPS	Delete file	<input checked="" type="checkbox"/>
FTP	Delete file	<input type="checkbox"/>

Scan Exceptions help

Skip if the file or message is larger than 10240 KB (Maximum: 51200 KB)

Back Next Cancel

Figure 2-14

Enter the settings as explained in [Table 2-4](#), then click **Next** to go the following screen.


 **Note:** After you have completed the steps in the Setup Wizard, you can make changes to the Web security settings by selecting **Web Security > Policy** or **Web Security > HTTP/HTTPS > Malware Scan**. The Malware Scan screen also lets you specify HTML scanning and notification settings. For more information about these settings, see [“Configuring Web and Services Protection”](#) on page 4-22.

Table 2-4. Setup Wizard Step 5: Web Security Settings

Setting	Description (or Subfield and Description)	
Services to Scan		
HTTP	HTTP scanning is enabled by default on standard service port 80.	To disable Hypertext Transfer Protocol (HTTP) scanning, deselect the corresponding checkbox. You can change the standard service port or add another port in the corresponding Ports to Scan field.

Table 2-4. Setup Wizard Step 5: Web Security Settings (continued)

Setting	Description (or Subfield and Description)	
HTTPS	HTTPS scanning is disabled by default.	To enable Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) scanning, select the corresponding checkbox. You can change the standard service port (port 443) or add another port in the corresponding Ports to Scan field.
FTP	FTP scanning is enabled by default on standard service port 21.	To disable File Transfer Protocol (FTP) scanning, deselect the corresponding checkbox. You can change the standard service port or add another port in the corresponding Ports to Scan field.
Scan Action		
HTTP	<p>From the HTTP pull-down menu, specify one of the following actions when an infected Web file or object is detected:</p> <ul style="list-style-type: none"> • Quarantine file. The Web file or object is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or spyware log entry. • Delete file. This is the default setting. The Web file or object is deleted, and a virus log entry or spyware log entry is created. • Log only. Only a virus log entry or spyware log entry is created. The Web file or object is not deleted. <p>Select the Streaming checkbox to enable streaming of partially downloaded and scanned HTTP file parts to the end user. This method allows the user to experience more transparent Web downloading. Streaming is enabled by default.</p>	
HTTPS	<p>From the HTTPS pull-down menu, specify one of the following actions when an infected Web file or object is detected:</p> <ul style="list-style-type: none"> • Quarantine file. The Web file or object is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or spyware log entry. • Delete file. This is the default setting. The Web file or object is deleted, and a virus log entry or spyware log entry is created. • Log only. Only a virus log entry or spyware log entry is created. The Web file or object is not deleted. <p>Select the Streaming checkbox to enable streaming of partially downloaded and scanned HTTPS file parts to the end user. This method allows the user to experience more transparent Web downloading. Streaming is enabled by default.</p>	

Table 2-4. Setup Wizard Step 5: Web Security Settings (continued)

Setting	Description (or Subfield and Description)
FTP	<p>From the FTP pull-down menu, specify one of the following actions when an infected Web file or object is detected:</p> <ul style="list-style-type: none"> • Quarantine file. The Web file or object is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or spyware log entry. • Delete file. This is the default setting. The Web file or object is deleted, and a virus log entry or spyware log entry is created. • Log only. Only a virus log entry or spyware log entry is created. The Web file or object is not deleted.
Scan Exceptions	
<p>From the pull-down menu, specify one of the following actions when a Web file or object exceeds the size that you specify in the file size field:</p> <ul style="list-style-type: none"> • Skip. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • Block. The file is blocked and does not reach the end user. <p>The default and maximum file sizes are:</p> <ul style="list-style-type: none"> • For the STM600 and STM300, the default setting is to block any attachment larger than 10240 KB. The maximum file size that you can specify is 51200 KB. • For the STM150, the default setting is to block any attachment larger than 8192 KB. The maximum file size that you can specify is 25600 KB. <p>Note: Setting the maximum file size to a high value might affect the STM's performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats.</p>	

Setup Wizard Step 6 of 11: Email Notification Server Settings

The screenshot shows the 'Email Notification Server' configuration window. The title bar reads 'Step 6 of 11: Email Notification Server'. The window has a 'help' icon in the top right. The configuration fields are as follows:

- Show as Mail Sender:
- Send Notifications to: (Example: admin@yourdomain.com)
- SMTP Server: :
- Mail Server Requires Authentication
- User Name:
- Password:

At the bottom of the window are three yellow buttons: 'Back', 'Next', and 'Cancel'.

Figure 2-15

Enter the settings as explained in [Table 2-5 on page 2-20](#), then click **Next** to go the following screen.


	<p>Note: After you have completed the steps in the Setup Wizard, you can make changes to the administrator e-mail notification settings by selecting Global Settings > Email Notification server. For more information about these settings, see “Configuring the E-mail Notification Server” on page 6-2.</p>
---	---

Table 2-5. Setup Wizard Step 6: Email Notification Server Settings

Setting	Description (or Subfield and Description)	
Email Notification Server Settings		
Show as Mail sender	A descriptive name of the sender for e-mail identification purposes. For example, enter stm600notification@netgear.com.	
Send Notifications to	The e-mail address to which the notifications should be sent. Typically, this is the e-mail address of a user with administrative privileges.	
SMTP server	The IP address and port number or Internet name and port number of your ISP's outgoing e-mail SMTP server. The default port number is 25. Note: If you leave this field blank, the STM cannot send e-mail notifications.	
Mail Server Requires Authentication	If the SMTP server requires authentication, select the Mail Server Requires Authentication checkbox and enter the following settings:	
	User Name	The user name for SMTP server authentication.
	Password	The password for SMTP server authentication.

Setup Wizard Step 7 of 11: Update Settings

Step 7 of 11: Update Settings

System Information help

Component	Current Version	Last Update
Software	V2.0.0-23	2009-08-12
Scan Engine	V5.5.4.171	2009-05-05
Pattern File	200909181747	2009-09-18
OS	V1.1.0.31	2009-06-05

Update Settings help

Update From

Default Update Server

Another Update Server

Server Address:

Update Component

Update Signature Patterns only

Update all Software and Signature Patterns

Update Frequency help

Weekly: Sunday : 23 : 00 (hh:mm)

Daily: 01 : 00 (hh:mm)

Every: 1 hour

Back **Next** **Cancel**

Figure 2-16

Enter the settings as explained in [Table 2-6 on page 2-22](#), then click **Next** to go the following screen.



Note: After you have completed the steps in the Setup Wizard, you can make changes to the security subscription update settings by selecting **Administration > Software Update**. For more information about these settings, see [“Updating the Software” on page 3-19](#).

Table 2-6. Setup Wizard Step 7: Update Settings

Setting	Description (or Subfield and Description)		
System Information			
You cannot configure this section; it is shown for information only. For the software, Scan Engine, (signature) Pattern File, and operating system (OS), the current version and the date of the last update are displayed.			
Update Settings			
Update From	<p>Select one of the following radio buttons:</p> <ul style="list-style-type: none"> • Default update server. The scan engine and signatures are updated from the NETGEAR default update server. • Another Server address. The scan engine and signatures are updated from a server that you specify by entering the server IP address or host name in the Server Address field. 		
	<table border="1"> <tr> <td>Server Address</td> <td>The update server IP address or host name.</td> </tr> </table>	Server Address	The update server IP address or host name.
Server Address	The update server IP address or host name.		
Update Component	<p>Make one of the following selections from the pull-down menu:</p> <ul style="list-style-type: none"> • Update Signature Patterns only. Only the (signature) Pattern File is updated. The software, Scan Engine, and OS are not updated. • Update all Software and Signature Patterns. The software, Scan Engine, (signature) Pattern File, and OS are updated. This is the default setting. 		
Update Frequency			
<p>Make one of the following selections:</p> <ul style="list-style-type: none"> • Weekly. From the pull-down menus, specify the day, hour, and minutes that the update should occur. • Daily. From the pull-down menus, specify the hour and minutes that the update should occur. • Every. From the pull-down menus, specify the frequency with which the update should occur. 			

Setup Wizard Step 8 of 11: HTTP Proxy Settings

Figure 2-17

Enter the settings as explained in [Table 2-7](#), then click **Next** to go the following screen.

	<p>Note: After you have completed the steps in the Setup Wizard, you can make changes to the security subscription update settings by selecting Global Settings > HTTP Proxy. For more information about these settings, see “Configuring the HTTP Proxy Settings” on page 3-7.</p>
--	--

Table 2-7. Setup Wizard Step 8: HTTP Proxy Settings

Setting	Description (or Subfield and Description)
HTTPS Proxy Settings	
Use a Proxy Server to Connect to the Internet	If computers on the network connect to the Internet via a proxy server, select the Use a Proxy Server to Connect to the Internet checkbox to specify and enable a proxy server. Enter the following settings:
Proxy Server	The IP address and port number of the proxy server.
User Name	The user name for proxy server authentication.
Password	The password for proxy server authentication.

Setup Wizard Step 9 of 11: Web Categories



Figure 2-18

Enter the settings as explained in [Table 2-8](#), then click **Next** to go the following screen.


	<p>Note: After you have completed the steps in the Setup Wizard, you can make changes to the content filtering settings by selecting Web Security > HTTP/HTTPS > Content Filtering. The Content Filtering screen lets you specify additional filtering tasks and notification settings. For more information about these settings, see “Configuring Web Content Filtering” on page 4-26.</p>
---	--

Table 2-8. Setup Wizard Step 9: Web Categories Settings

Setting	Description (or Subfield and Description)
Select the Web Categories You Wish to Block	
<p>Select the Enable Blocking checkbox to enable blocking of Web categories, which is the default setting. Select the checkboxes of any Web categories that you want to block. Use the action buttons in the following way:</p> <ul style="list-style-type: none"> • Allow All. All Web categories are allowed. • Block All. All Web categories are blocked. • Set to Defaults. Blocking and allowing of Web categories are returned to their default settings. See Table 4-1 on page 4-2 for information about the Web categories that are blocked by default. Categories that are preceded by a green rectangular are allowed by default; categories that are preceded by a pink rectangular are blocked by default. 	

Setup Wizard Step 10 of 11: Configuration Summary

Step 10 of 11: Configuration Summary

Network Settings

System Name: STM600
 IP Address: 192.168.1.161
 Subnet Mask: 255.255.255.0
 Gateway IP Address: 192.168.1.254
 Primary DNS: 192.168.1.254
 Secondary DNS: 4.2.2.2
 Maximum Transmission Unit: 1500

System Date and Time

Use NTP Server: time-g.netgear.com,time-h.netgear.com
 Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Email Security

Status	Service	Ports To Scan	Action
Enable	SMTP	25	Block infected email
Enable	POP3	110	Delete attachment
Enable	IMAP	143	Delete attachment
Skip if a file or message is larger than:			10240 KB

Web Security

Status	Service	Ports To Scan	Action
Enable	HTTP	80	Delete file (Streaming)
Disable	HTTPS	443	Delete file (Streaming)
Enable	FTP	21	Delete file
Skip if a file or message is larger than:			10240 KB

Email Notification Server

Emails Sent As: stm600notification@netgear.com
 SMTP Server: 123.456.0.789
 Mail Recipients: admin@yourdomain.com

Update Settings

Update Server Address: update1.beta.netgear.com
 Update Component: Software and pattern
 Frequency: 1h

HTTP Proxy Settings

HTTP Proxy: Disable
 Proxy Server:

Blocked Web Categories

<input checked="" type="checkbox"/> Alcohol & Tobacco	<input checked="" type="checkbox"/> Anonymizers	<input checked="" type="checkbox"/> Botnets
<input checked="" type="checkbox"/> Child Abuse Images	<input checked="" type="checkbox"/> Criminal Activity	<input checked="" type="checkbox"/> Gambling
<input checked="" type="checkbox"/> Games	<input checked="" type="checkbox"/> Hacking	<input checked="" type="checkbox"/> Hate & Intolerance
<input checked="" type="checkbox"/> Illegal Drug	<input checked="" type="checkbox"/> Illegal Software	<input checked="" type="checkbox"/> Malware
<input checked="" type="checkbox"/> Nudity	<input checked="" type="checkbox"/> Phishing & Fraud	<input checked="" type="checkbox"/> Pornography / Sexually Explicit
<input checked="" type="checkbox"/> School Cheating	<input checked="" type="checkbox"/> Sex Education	<input checked="" type="checkbox"/> Spam Sites
<input checked="" type="checkbox"/> Tasteless	<input checked="" type="checkbox"/> Uncategorized	<input checked="" type="checkbox"/> Violence
<input checked="" type="checkbox"/> Virus Infected / Compromised	<input checked="" type="checkbox"/> Weapons	

New settings will be applied after you click the 'Apply' button. System reboot is required for the new settings take effect. When the appliance finishes rebooting, please make sure it has Internet access and register management interface to activate your license keys or free trial.

Back
Apply
Cancel

Figure 2-19

Click **Apply** to save your settings and automatically restart the system or click **Back** to make changes to the configuration.

Setup Wizard Step 11 of 11: Restarting the System

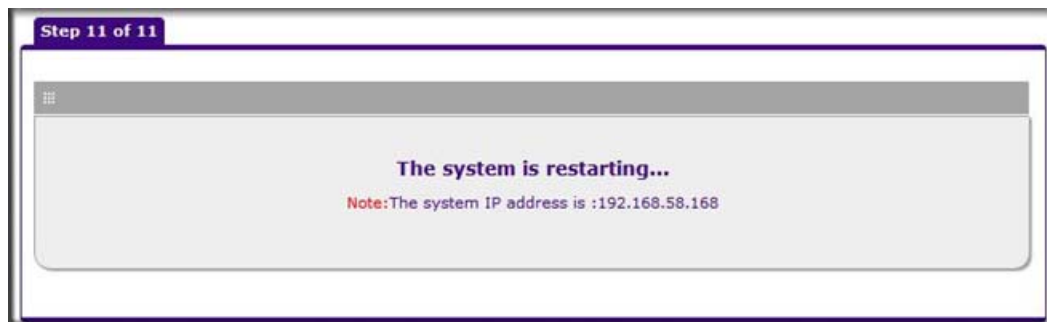


Figure 2-20

Wizard screen 11 is just an informational screen to let you know that the S restarts automatically with the new configuration.

Verifying Proper Installation

Test the STM before deploying it in a live production environment. The following instructions walk you through a couple of quick tests designed to ensure that your STM is functioning correctly.

Testing Connectivity

Verify that network traffic can pass through the STM:

- Ping an Internet URL.
- Ping the IP address of a device on either side of the STM.

Testing HTTP Scanning

If client computers have direct access to the Internet through your LAN, try to download the eicar.com test file from <http://www.eicar.org/download/eicar.com>.

The eicar.com test file is a legitimate DoS program and is safe to use because it is not a malware threat and does not include any fragments of malware code. The test file is provided by EICAR, an organization that unites efforts against computer crime, fraud, and misuse of computers or networks.

Verify that the STM properly scans HTTP traffic:

1. Log in to the STM Web Management Interface, and then verify that HTTP scanning is enabled. For information about how to enable HTTP scanning, see [“Customizing Web Protocol Scan Settings” on page 4-22](#).
2. Check the downloaded eicar.com test file, and note the attached malware information file.

Registering the STM with NETGEAR

To receive threat management component updates and technical support, you must register your STM with NETGEAR. The support registration keys are provided with the product package (see [“Service Registration Card with License Keys” on page 1-6](#)).

The STM supports a Bundle Key, which is a single support registration key that provides all three licenses: Web protection, Email protection, and Support & Maintenance.



Note: Activating the service licenses initiates their terms of use. Activate the licenses only when you are ready to start using this unit. If your unit has never been registered before you can use the 30-day trial period for all 3 types of licenses to perform the initial testing and configuration. To use the trial period, do not click Register in [step 4](#) of the procedure below but click **Trial** instead.

If your STM is connected to the Internet, you can activate the service licenses:

1. Select **Support > Registration** from the menu. The Registration screen displays (see [Figure 2-21 on page 2-29](#)).

Registration Key:

License Key	License Type	Expiration Date
NG2002-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	Web Protection	2010-07-21
NG2001-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	Email Protection	2010-07-21
NG2000-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	Support & Maintenance	2010-07-21

Customer Information

Company Name:

First Name:

Last Name:

Email Address:

Fax Number:

Phone Number:

Address:

Country:

VAR Information

Company Name:

First Name:

Last Name:

Email Address:

Fax Number:

Phone Number:

Address:

Country:

Figure 2-21

2. Enter the license key in the Registration Key field.
3. Fill out the customer and VAR fields.
4. Click **Register**.
5. Repeat [step 2](#) and [step 4](#) for additional license keys.

The STM activates the licenses and registers the unit with the NETGEAR registration server.



Note: When you reset the STM to the original factory default settings after you have entered the license keys to activate the STM (see [“Registering the STM with NETGEAR” on page 2-28](#)), the license keys are erased. The license keys and the different types of licenses that are available for the STM are no longer displayed on the Registration screen. However, after you have reconfigured the STM to connect to the Internet and to the NETGEAR registration server, the STM retrieves and restores all registration information based on its MAC address and hardware serial number. You do not need to re-enter the license keys and re-activate the STM.

What to Do Next

You have completed setting up and deploying the STM to the network. The STM is now set up to scan the protocols and services that you specified for malware threats and to perform updates based on the configured update source and frequency.

If you need to change the settings, or to view reports or logs, log in to the STM Web Management Interface, using the default IP address or the IP address that you assigned to the STM in [“Setup Wizard Step 1 of 10: Introduction” on page 2-10](#).

The STM is ready for use. However, some important tasks that you might want to address before you deploy the STM in your network are listed below:

- [“Changing Administrative Passwords and Timeouts” on page 3-9](#).
- [“Managing Digital Certificates” on page 3-25](#).
- [“Configuring Groups” on page 5-2](#).
- [“Configuring User Accounts” on page 5-6](#).
- [“Configuring Authentication” on page 5-9](#).
- [“Setting Scanning Exclusions and Web Access Exceptions” on page 4-46](#).

Chapter 3

Performing Network and System Management

This chapter describes the network settings, the system management features, and ways to improve the performance of the STM. If you have used the Setup Wizard, you have already configured some of these settings, but there are situations in which you might want to modify them. This chapter contains the following sections:

- [“Configuring Network Settings”](#) on this page.
- [“Configuring Session Limits and Timeouts”](#) on page 3-5.
- [“Configuring the HTTP Proxy Settings”](#) on page 3-7.
- [“About Users with Administrative and Guest Privileges”](#) on page 3-9.
- [“Configuring Remote Management Access”](#) on page 3-11.
- [“Using an SNMP Manager”](#) on page 3-13.
- [“Managing the Configuration File”](#) on page 3-16.
- [“Updating the Software”](#) on page 3-19.
- [“Configuring Date and Time Service”](#) on page 3-23
- [“Managing Digital Certificates”](#) on page 3-25
- [“Managing the Quarantine Settings”](#) on page 3-30
- [“Performance Management”](#) on page 3-31.

Configuring Network Settings

If you have used the Setup Wizard, you might already have configured the Web Management Interface and maximum transmission unit (MTU) settings; the Network Settings screen allows you to modify these settings and to specify the interface speed and duplex settings.

The STM requires a valid IP address to retrieve online updates and to enable access to its Web Management Interface. If you have used the Setup Wizard to configure the STM, you have already specified the the management interface name and address settings and the size of the MTU. In addition to modifying these settings, the Network Settings screen also allows you to specify the interface speed and duplex settings for the management interface, for the STM600 or STM300 uplink and downlink interfaces, or for the STM150’s WAN and LAN interfaces.

To configure the STM's network settings:

1. Select **Global Settings > Network Settings** from the menu. The Network Settings submenu tabs appear with the Network Settings screen in view (Figure 3-1 shows the STM600).

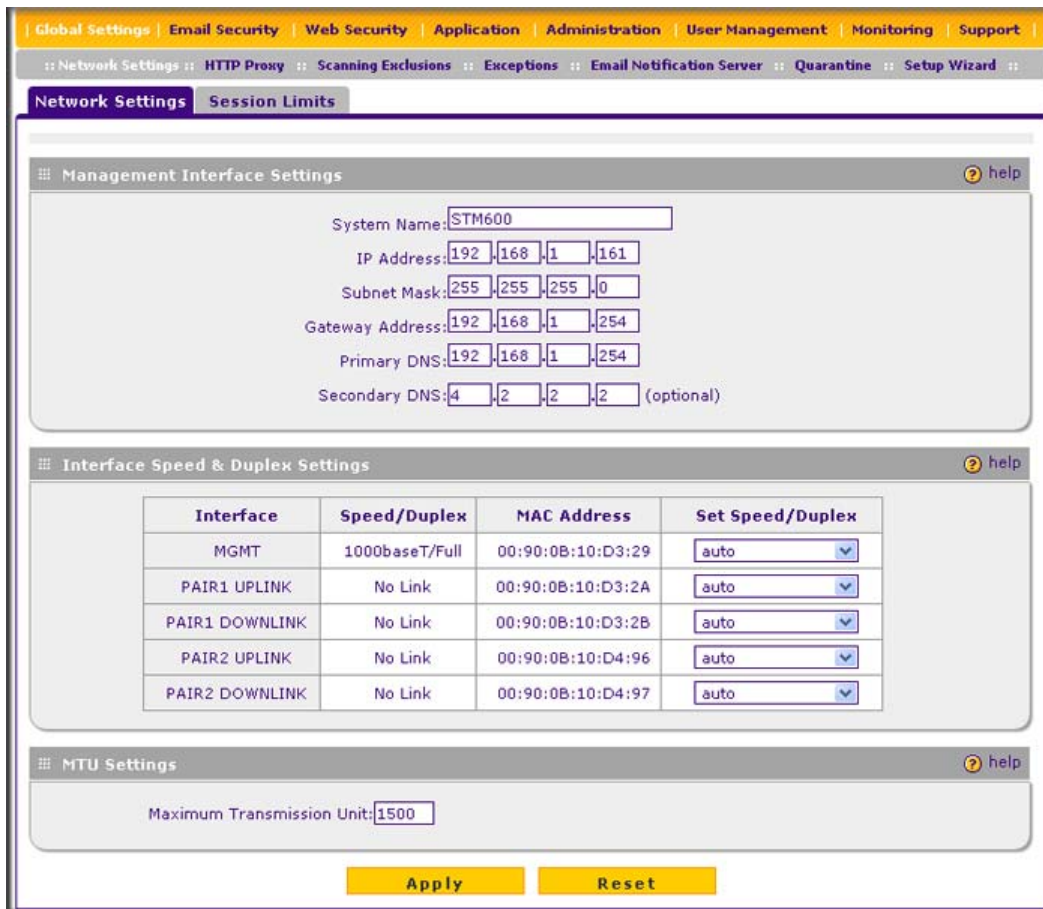


Figure 3-1 [STM600]

Figure 3-2 on page 3-3 shows the Interface Speed & Duplex Settings section of the Network Settings screen of the STM300.

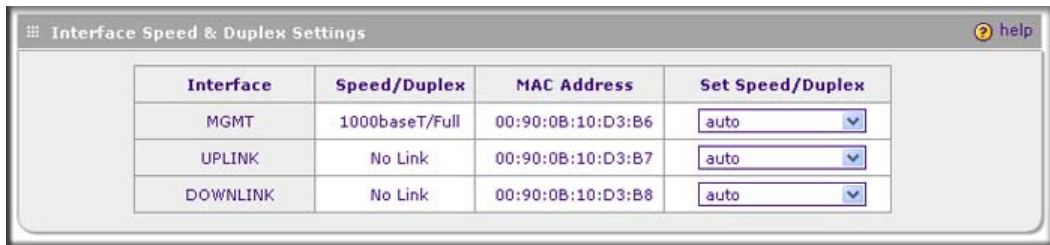


Figure 3-2 [STM300]

Figure 3-3 shows the Interface Speed & Duplex Settings section of the Network Settings screen of the STM150.

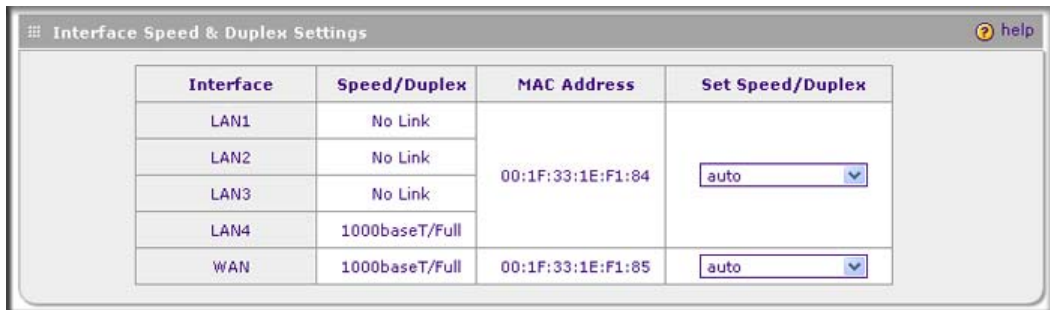


Figure 3-3 [STM150]

- Complete the fields and make your selections from the pull-down menus as explained in Table 3-1.

Table 3-1. Network Settings

Setting	Description (or Subfield and Description)
Management Interface Settings	
System Name	The name for the STM for purposes of identification and management. The default name is the name of your model (STM150, STM300, or STM600).
IP Address	Enter the IP address of the STM through which you will access the Web Management Interface. The factory default IP address is 192.168.1.201. Note: If you change the IP address of the STM while being connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again. For example, if you change the default IP address from 192.168.1.201 to 10.0.0.1, you must now enter https://10.0.0.1 in your browser to reconnect to the Web Management Interface.

Table 3-1. Network Settings (continued)

Setting	Description (or Subfield and Description)	
Subnet Mask	Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask.	
Gateway Address	Enter the IP address of the gateway through which the STM is accessed.	
Primary DNS	Specify the IP address for the primary DNS server IP address.	
Secondary DNS	As an option , specify the IP address for the secondary DNS server IP address.	
<p>Interface Speed & Duplex Settings</p> <p>These sections show for each interface the MAC address, and for each active interface the assigned speed and duplex setting. The Set Speed/Duplex pull-down menu allows you to select the speed and duplex setting for each active interface. To set the speed to 1000baseT duplex (“full”), select auto to let the STM sense the speed automatically.</p> <p>Note: MGMT stands for management interface.</p>		
STM600 (see Figure 3-1 on page 3-2)	MGMT	From the Set Speed/Duplex pull-down menu, make one of the following selections: <ul style="list-style-type: none"> • auto. Speed autosensing This is the default setting. • 10baseT/Half. Ethernet speed at half duplex. • 10baseT/Full. Ethernet speed at full duplex. • 100baseT/Half. Fast Ethernet speed at half duplex. • 100baseT/Full. Fast Ethernet speed at full duplex.
	PAIR1 UPLINK	
	PAIR1 DOWNLINK	
	PAIR2 UPLINK	
	PAIR2 DOWNLINK	
STM300 (see Figure 3-2 on page 3-3)	MGMT	From the Set Speed/Duplex pull-down menu, make one of the following selections: <ul style="list-style-type: none"> • auto. Speed autosensing This is the default setting. • 10baseT/Half. Ethernet speed at half duplex. • 10baseT/Full. Ethernet speed at full duplex. • 100baseT/Half. Fast Ethernet speed at half duplex. • 100baseT/Full. Fast Ethernet speed at full duplex.
	UPLINK	
	DOWNLINK	
STM150 (see Figure 3-3 on page 3-3)	LAN1 LAN2 LAN3 LAN4	From the Set Speed/Duplex pull-down menu, make one of the following selections: <ul style="list-style-type: none"> • auto. Speed autosensing. This is the default setting, which can sense 1000BaseT speed at full duplex. • 10baseT/Half. Ethernet speed at half duplex. • 10baseT/Full. Ethernet speed at full duplex. • 100baseT/Half. Fast Ethernet speed at half duplex. • 100baseT/Full. Fast Ethernet speed at full duplex. <p>Note: All LAN interfaces share the same MAC address, speed, and duplex mode.</p> <p>Note: The STM150 does not provide a dedicated management interface.</p>
	WAN	

Table 3-1. Network Settings (continued)

Setting	Description (or Subfield and Description)
MTU Settings	
Maximum Transmission Unit	The maximum transmission unit (MTU) is the largest physical packet size that a network can transmit. Packets that are larger than the MTU value are divided into smaller packets before they are sent, an action that prolongs the transmission process. For most Ethernet networks the MTU value is 1500 Bytes, which is the default setting. Note: NETGEAR recommends synchronizing the STM's MTU setting with that of your network to prevent delays in transmission.

- Click **Apply** to save your settings. Changing the network settings has the following consequences:
 - Changing any of the settings in the Management Interface Settings section of the screen causes the STM to restart.
 - Changing any of the settings in the Interface Speed & Duplex Settings section of the screen causes the network to restart.
 - Changing the MTU setting causes services such as HTTP and SMTP to restart.

If you click **Reset**, the STM restarts to restore the default network settings.

Configuring Session Limits and Timeouts

The Session Limits screen allows you to specify the total number of sessions per user (that is, per IP address or single source machine) that are allowed on the STM. Session limiting is disabled by default. When session limiting is enabled, you can specify the maximum number of sessions per user either as an absolute number or as a percentage of the STM's total connection capacity per user, which is 10000 sessions. (You cannot change the total connection capacity per user.) If a user exceeds the number of allocated sessions, packets might be dropped.



Note: Some protocols such as FTP and RSTP create two sessions per connection.

To configure session limits and timeouts:

- Select **Global Settings > Network Settings** from the menu. The Network Settings submenu tabs appear with the Network Settings screen in view.

- Click the **Session Limits** submenu tab. The Session Limits screen displays.

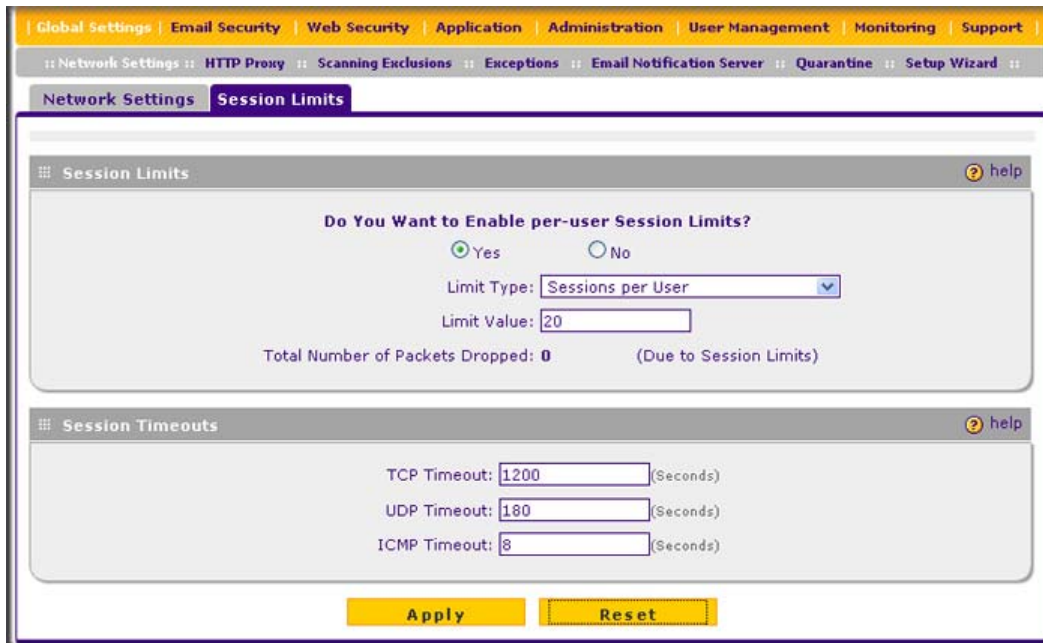


Figure 3-4

- Select the radio buttons, make your selections from the pull-down menu, and complete the fields as explained in [Table 3-2](#).

Table 3-2. Session Limits Settings

Setting	Description (or Subfield and Description)
Session Limits	
Do You Want to Enable per-user Session Limits?	Select the Yes radio button to enable session limits, and then specify the Limit Type and Limit Value fields. The No radio button is selected by default.
Limit Type	From the Limit Type pull-down menu, make one of the following selections: <ul style="list-style-type: none"> • Percentage of Maximum Sessions. Session limits are set as a percentage of the the total connection capacity per user. • Sessions per User. Session limits are set as an absolute number.

Table 3-2. Session Limits Settings (continued)

Setting	Description (or Subfield and Description)	
Do You Want to Enable per-user Session Limits? (continued)	Limit Value	Depending on the selection in the Limit Type field, this value is a percentage or an absolute number.
	The Total Number of Packets Dropped field, which you cannot configure, shows the total number of packets that are dropped because the session limit has been exceeded.	
Session Timeouts If a session goes without data flow longer than the configured values, the session is terminated.		
TCP Timeout	The time in seconds after which a TCP session without data flow is terminated. The default time is 1200 seconds.	
UDP Timeout	The time in seconds after which an UDP session without data flow is terminated. The default time is 180 seconds.	
ICMP Timeout	The time in seconds after which an ICMP session without data flow is terminated. The default time is 8 seconds.	

- Click **Apply** to save your settings. Changing any settings in the Session Timeouts section of the screen requires the STM to restart. If you click **Reset**, the STM restarts to restore the default network settings.

Configuring the HTTP Proxy Settings

If you have used the Setup Wizard, you might have already configured an HTTP proxy; the HTTP Proxy screen allows you to modify these settings.

If the STM is installed behind an HTTP proxy, you might need to specify the HTTP proxy settings for the STM to connect to the Internet. The settings on the HTTP Proxy screen affect Web category filtering, Distributed Spam Analysis, and software updates.

To configure the HTTP proxy:

1. Select **Global Settings > HTTP Proxy** from the menu. The HTTP Proxy screen displays.

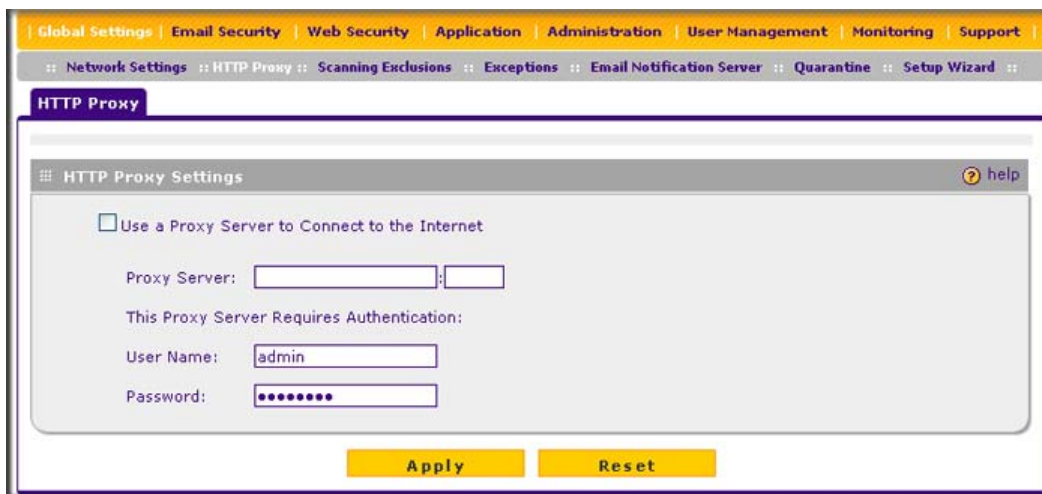


Figure 3-5

2. Select the checkbox and complete the fields as explained in [Table 3-3](#).

Table 3-3. HTTP Proxy Settings

Setting	Description (or Subfield and Description)	
HTTPS Proxy Settings		
Use a Proxy Server to Connect to the Internet	If computers on the network connect to the Internet via a proxy server, select the Use a Proxy Server to Connect to the Internet checkbox to specify and enable a proxy server. Enter the following settings:	
	Proxy Server	The IP address and port number of the proxy server.
	User Name	The user name for proxy server authentication.
	Password	The password for proxy server authentication.

3. Click **Apply** to save your settings.

About Users with Administrative and Guest Privileges

There are two pre-defined user types that can access the STM's Web Management Interface:

- **Administrator.** A user who has full access and the capacity to change the STM configuration (that is, read/write access). The default user name for an administrator is **admin**, and the default password for an administrator is **password**.
- **Guest user.** A user who can only view the STM configuration (that is, read-only access). The default user name for a guest is **guest**, and the default password for a guest is **guest**.

NETGEAR recommends that you change these passwords to more secure passwords.

The login window that is presented to the administrator and guest user is the NETGEAR Configuration Manager Login screen (see [Figure 5-6 on page 5-9](#)).

Changing Administrative Passwords and Timeouts

In addition to changing the default password for the administrator and guest user, you can use the Set Password screen to change the account names, and modify the Web Management Interface timeout setting.



Note: The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. The password can be up to 64 characters.

To modify the administrator and guest accounts, and to modify the Web Management Interface timeout setting:

1. Select **Administration > Set Password** from the menu. The Set Password screen displays (see [Figure 3-6 on page 3-10](#)).

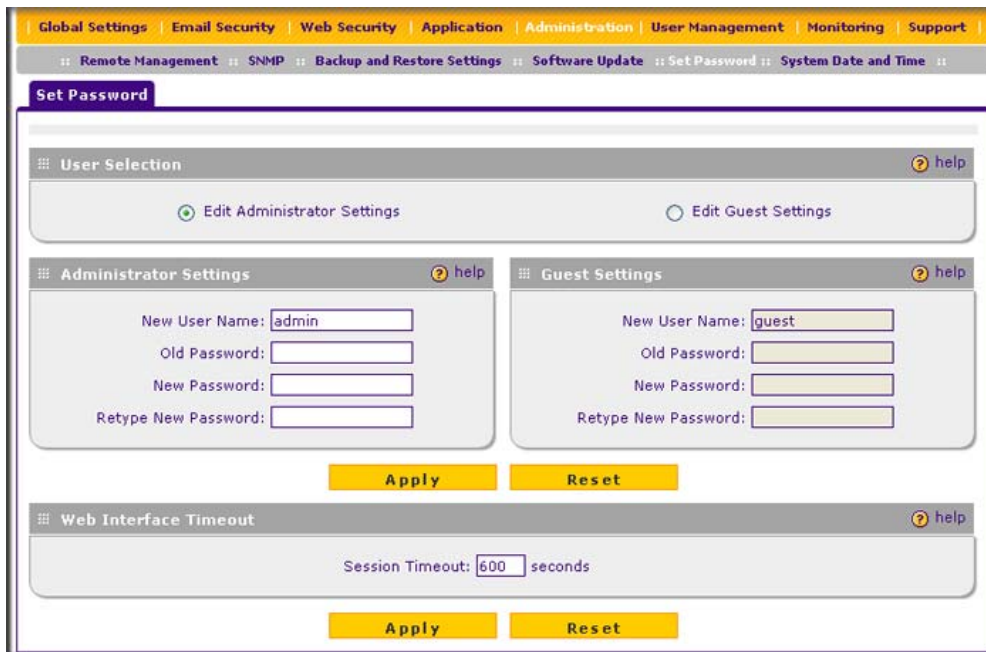


Figure 3-6

- To modify the administrator or guest settings, select the checkbox and complete the fields as explained in [Table 3-4](#).

Table 3-4. Set Password Settings screen; Administrator and Guest Settings

Setting	Description (or Subfield and Description)
User Selection	
Select one of the following radio buttons:	
<ul style="list-style-type: none"> • Edit Administrator Settings. Allows you to modify the administrator settings, while the guest settings are masked out. • Edit Guest Settings. Allows you to modify the guest settings, while the administrator settings are masked out. 	
Administrator Settings/Guest Setting	
New User Name	The default user name. For the administrator account, the default name is admin; for the guest account, the default name is guest.
Old Password	The current (factory default) password
New Password	Enter the new password.
Retype New Password	Confirm the new password.

3. Under the Administrator Settings and Guest Settings sections of the screen, click **Apply** to save your settings.
4. If you modified the administrator settings and now want to modify the guest settings, or the other way around, repeat [step 2](#) and [step 3](#) for the other settings.
5. To modify the Web Management Interface timeout settings, complete the field as explained in [Table 3-5](#).

Table 3-5. Set Password Settings screen: Web Interface Timeout Settings

Setting	Description (or Subfield and Description)
Web Interface Timeout	
Session Timeout	Enter the period in seconds after which the Web Management Interface is automatically logged off if no activity is detected. The default is 600 seconds. You can configure a session timeout from 30 seconds to 9999 seconds.

6. Under the Web Interface Timeout section of the screen, click **Apply** to save your settings.



Note: After a factory default reset, the password and timeout value are changed back to **password** and 600 seconds (5 minutes), respectively.

Configuring Remote Management Access

An administrator can configure, upgrade, and check the status of the STM over the Internet via a Secure Sockets Layer (SSL) VPN connection.

You must use an SSL VPN connection to access the STM from the Internet. You must enter *https://* (not *http://*) and type the STM's WAN IP address into your browser. For example, if the STM's WAN IP address is 172.16.0.123, type the following in your browser: **https://172.16.0.123**.

The STM's remote login URL is:

https://<IP_address> or **https://<FullyQualifiedDomainName>**



Note: The STM is accessible to anyone who knows its IP address and default password. Because a malicious WAN user can reconfigure the STM and misuse it in many ways, NETGEAR highly recommends that you change the admin and guest default passwords before continuing (see [“Changing Administrative Passwords and Timeouts”](#) on page 3-9).

To configure remote management:

1. Select **Administration** > **Remote Management** from the menu. The Remote Management screen displays (see [Figure 3-7](#) on page 3-12).

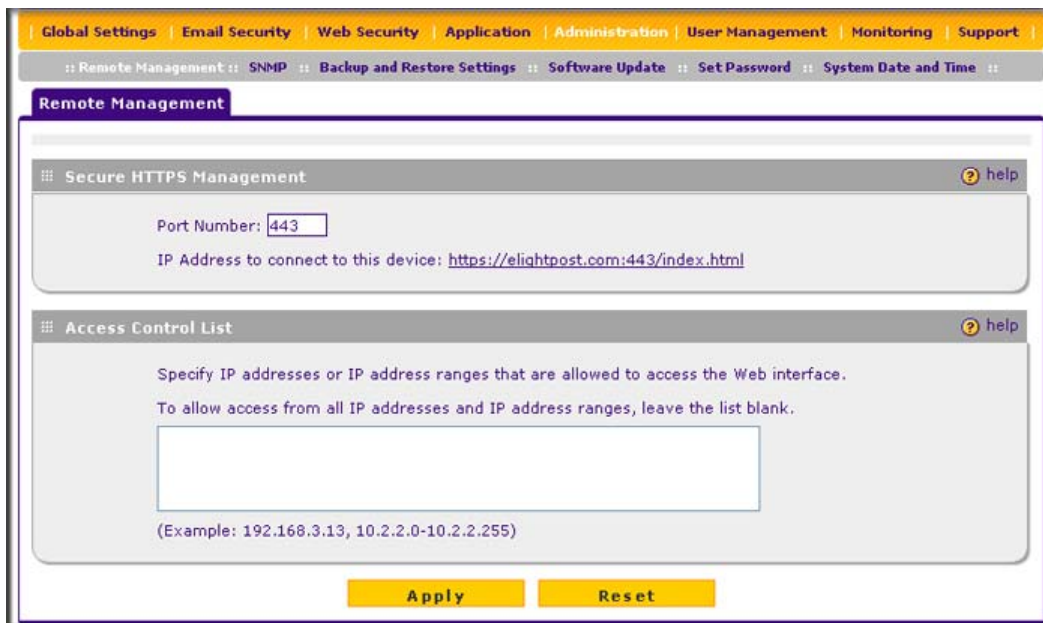


Figure 3-7

2. In the Secure HTTPS Management section of the screen, enter number of the port that you want to use to access Web Management Interface of the STM. The default setting is port 443, but you can enter a port ranging from 1024 to 65535. You cannot use some ports such as 2080 and 8088 that might be used by the STM.

This section of the screen also displays the HTTPS hyperlink through which you can access the Web Management Interface of the STM. The hyperlink consists of the IP address or fully qualified domain name (FQDN) for the STM and the port number that you have assigned.

3. In the Access Control List section of the screen, you can specify IP addresses or IP address ranges that you want to grant access to the Web Management Interface for increased security. To specify a range, separate the beginning IP address and the ending IP address by a dash (-). To allow access from all IP addresses and IP address ranges, leave this field blank.
4. Click **Apply** to save your changes.



Note: To maintain security, the STM rejects a login that uses *http://address* rather than the SSL *https://address*.



Note: The first time that you remotely connect to the STM with a browser via an SSL VPN connection, you might get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or higher, simply click Yes to accept the certificate.

Using an SNMP Manager

Simple Network Management Protocol (SNMP) forms part of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

SNMP lets you monitor and manage your STM from an SNMP manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. The STM provides support for report aggregation through SNMP version 1 (SNMPv1) and version 2 (SNMPv2).

To enable SNMP and to configure the SNMP settings:

1. Select **Administration** > **SNMP** from the menu. The SNMP screen displays (see [Figure 3-8 on page 3-14](#)).

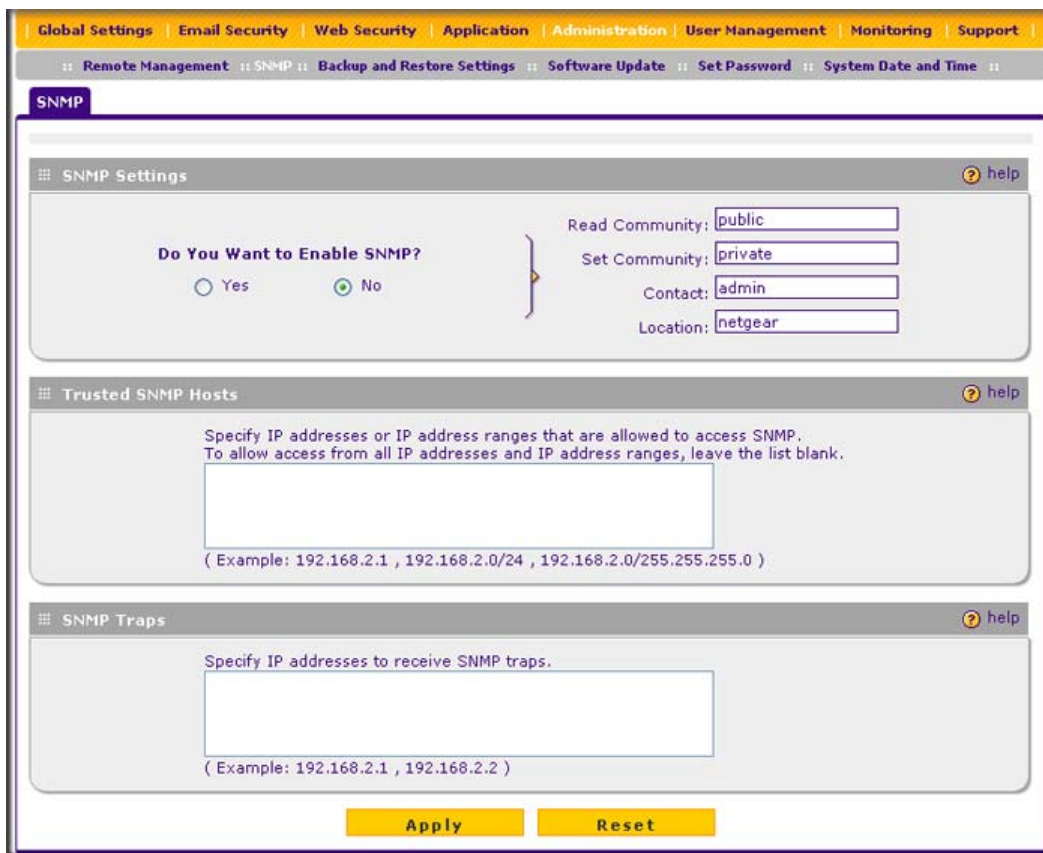


Figure 3-8

2. Select the radio buttons and complete the fields as explained in Table 3-6.

Table 3-6. SNMP Settings

Setting	Description (or Subfield and Description)
SNMP Settings	
Do You Want to Enable SNMP?	Select one of the following radio buttons: <ul style="list-style-type: none"> • Yes. Enable SNMP. • No. Disable SNMP. This is the default setting.
Read Community	The community string to allow an SNMP manager access to the MIB objects of the STM for the purpose of reading only. The default setting is public.

Table 3-6. SNMP Settings (continued)

Setting	Description (or Subfield and Description)	
Do You Want to Enable SNMP? (continued)	Set Community	The community string to allow an SNMP manager access to the MIB objects of the STM for the purpose of reading and writing. The default setting is private.
	Contact	The SNMP system contact information that is available to the SNMP manager. This setting is optional.
	Location	The physical location of the STM. This setting is optional.
Trusted SNMP Hosts		
Enter the IP addresses of the computers and devices to which you want to grant read-only ("GET") or write ("SET") privileges on the STM. Separate IP addresses by a comma. To allow any trusted SNMP host access, leave the field blank, which is the default setting.		
SNMP Traps		
Enter the IP addresses of the SNMP management stations that are allowed to receive the STM's SNMP traps. Separate IP addresses by a comma. If you leave the field blank, which is the default setting, no SNMP management station can receive the STM's SNMP traps.		

3. Click **Apply** to save your settings.

Supported MIB Browsers

After you have configured the SNMP settings, you must enter the IP address of the STM in the Management Information Base (MIB) browsers through which you want to query or configure the STM. See the documentation of your MIB browser for instructions.

NETGEAR recommends the following MIB browsers for receiving the STM SNMP notifications:

- MG-Soft
- SNMP
- Net-SNMP (Linux Text)
- SNMP Browser for KDE

The STM MIB structure is automatically downloaded by management stations. You should start receiving notifications after you have enabled SNMP on the STM and added its IP address into your MIB browsers.

Managing the Configuration File

The configuration settings of the STM are stored in a configuration file on the STM. This file can be saved (backed up) to a PC, retrieved (restored) from the PC, or cleared to factory default settings.

Once the STM is installed and works properly, make a back-up of the configuration file to a computer. If necessary, you can later restore the STM settings from this file. The Backup and Restore Settings screen lets you:

- back up and save a copy of the current settings
- restore saved settings from the backed-up file
- revert to the factory default settings.

To display the Backup and Restore Settings screen, select **Administration > Backup and Restore Settings** from the menu.

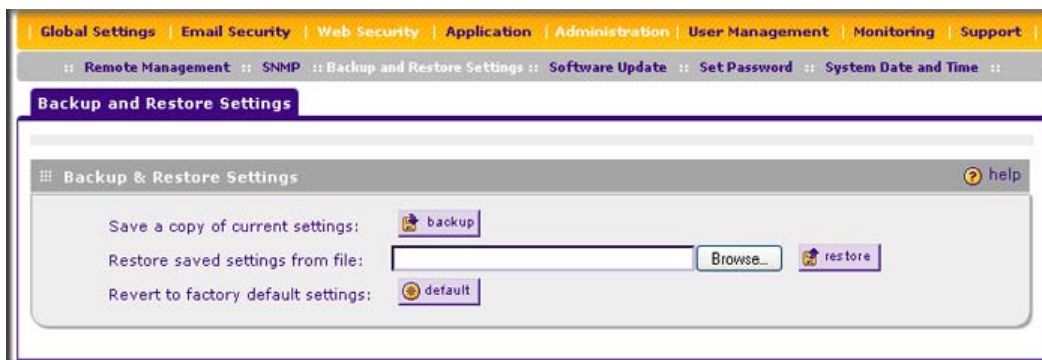


Figure 3-9

Backup Settings

The backup feature saves all STM settings to a file. These settings include:

- **Network settings.** IP address, subnet mask, gateway, and so on.
- **Scan settings.** Services to scan, primary and secondary actions, and so on.
- **Update settings.** Update source, update frequency, and so on.
- **Anti-spam settings.** Whitelist, blacklist, content filtering settings, and so on.

Back up your STM settings periodically, and store the backup file in a safe place.



Tip: You can use a backup file to export all settings to another STM that has the same language and management software versions. Remember to change the IP address of the second STM before deploying it to eliminate IP address conflicts on the network.

To backup settings:

1. On the Backup and Restore Settings screen (see [Figure 3-9 on page 3-16](#)), next to Save a copy of current settings, click the **backup** button to save a copy of your current settings. A dialog screen appears, showing the file name of the backup file (backup.gpg).
2. Select **Save file**, and then click **OK**.
3. Open the folder where you have saved the backup file, and then verify that it has been saved successfully.

Note the following:

- If your browser is not configured to save downloaded files automatically, locate the folder in which you want to save the file, specify the file name, and save the file.
- If you have your browser configured to save downloaded files automatically, the file is saved to your browser's download location on the hard disk.

Restore Settings



Warning: Restore only settings that were backed up from the same software version. Restoring settings from a different software version can corrupt your backup file or the STM system software.

To restore settings from a backup file:

1. On the Backup and Restore Settings screen (see [Figure 3-9 on page 3-16](#)), next to Restore save settings from file, click **Browse**.
2. Locate and select the previously saved backup file (by default, backup.pkg).
3. When you have located the file, click the **restore** button. A warning screen might appear, and you might have to confirm that you want to restore the configuration.

The STM restarts. During the reboot process, the Backup and Restore Settings screen remains visible. The reboot process is complete after several minutes when the Test LED on the front panel goes off.



Warning: Once you start restoring settings, do *not* interrupt the process. Do not try to go online, turn off the STM, shut down the computer, or do anything else to the STM until the settings have been fully restored.

Reverting to Factory Default Settings

To reset the STM to the original factory default settings, click the **default** button next to Revert to factory default settings on the Backup and Restore Settings screen (see [Figure 3-9 on page 3-16](#)).

The STM restarts. The Backup and Restore Settings screen remains visible during the reboot process. The reboot process is complete after several minutes when the Test LED (STM150) or Status LED (STM300 and STM600) on the front panel goes off.



Warning: When you restore the factory default settings, the STM settings are erased. All content settings and scan settings are lost. Back up your settings if you intend on using them.



Note: After rebooting with factory default settings, the STM administrator account password is **password**, the guest account password is **guest**, and the LAN IP address is **192.168.1.201**.



Note: For the STM150 only, there is an alternate way to return the settings to factory default: using a sharp object, press and hold the Reset button on the rear panel of the STM150 (see [“Rear Panel STM150” on page 1-14](#)) for about 10 seconds until the front panel Test LED flashes and the STM150 returns to factory default settings.

Updating the Software

If you have used the Setup Wizard, you might have already configured the software update settings; the Software Update screen allows you to modify these settings.

The STM has four main software components:

- The application software that includes the network protocols, security services, Web Management Interface, and other components.
- A scan engine that enables the STM to scan e-mails, attachments, Web files, and applications, and that functions in conjunction with the pattern file.
- A pattern file that contains the virus signature files and virus database.
- An operating system (OS) that includes the kernel modules and hardware drives.

The STM provides two methods for updating components:

- Scheduled, automatic update
- Manual update

Because new virus threats can appear any hour of the day, it is very important to keep both the pattern file and scan engine firmware as current as possible. The STM can automatically check for updates, as often as every 15 minutes, to ensure that your network protection is current.

Scheduling Updates

Enabling scheduled updates ensures that the STM automatically downloads the latest components from the NETGEAR update server.

To configure scheduled updates:

1. Select **Administration** > **Software Update** from the menu. The Software Update screen displays (see [Figure 3-10](#) on [page 3-20](#)).

Software Update

System Information help

Component	Current Version	Last Update
Software	V2.0.0-23	2009-08-12
Scan Engine	V5.5.4.171	2009-05-05
Pattern File	200909181747	2009-09-18
OS	V1.1.0.31	2009-06-05

Update Settings help

Update From

Default Update Server

Another Update Server

Server Address:

Update Component

Update Signature Patterns only

Update all Software and Signature Patterns

Update Frequency help

Weekly : : (hh:mm)

Daily : (hh:mm)

Every

Update Now **Apply** **Reset**

Figure 3-10

2. Select the radio buttons, complete the field, and make your selections from the pull-down menus as explained in [Table 3-7 on page 3-21](#).

Table 3-7. Software Update Settings

Setting	Description (or Subfield and Description)		
System Information			
You cannot configure this section; it is shown for information only. For the software, Scan Engine, (signature) Pattern File, and operating system (OS), the current version and the date of the last update are displayed.			
Update Settings			
Update From	Select one of the following radio buttons: <ul style="list-style-type: none"> • Default update server. The scan engine and signatures are updated from the NETGEAR default update server. • Another Server address. The scan engine and signatures are updated from a server that you specify by entering the server IP address or host name in the Server Address field. 		
	<table border="1"> <tr> <td>Server Address</td> <td>The update server IP address or host name.</td> </tr> </table>	Server Address	The update server IP address or host name.
Server Address	The update server IP address or host name.		
Update Component	Make one of the following selections from the pull-down menu: <ul style="list-style-type: none"> • Update Signature Patterns only. Only the (signature) Pattern File is updated. The software, Scan Engine, and OS are not updated. • Update all Software and Signature Patterns. The software, Scan Engine, (signature) Pattern File, and OS are updated. This is the default setting. 		
Update Frequency			
Make one of the following selections: <ul style="list-style-type: none"> • Weekly. From the pull-down menus, specify the day, hour, and minutes that the update should occur. • Daily. From the pull-down menus, specify the hour and minutes that the update should occur. • Every. From the pull-down menus, specify the frequency with which the update should occur. 			

3. Click **Apply** to save your settings.

Performing a Manual Update

If you want to immediately check for and download available updates, perform a manual update:

1. Select **Administration > Software Update** from the menu. The Software Update screen displays (see [Figure 3-10 on page 3-20](#)).
2. At the bottom of the screen, click **Update Now**. The STM contacts the update server and checks for available updates. If updates are available, the Update Progress screen appears to show the progress of the update (see [Figure 3-11 on page 3-22](#)).

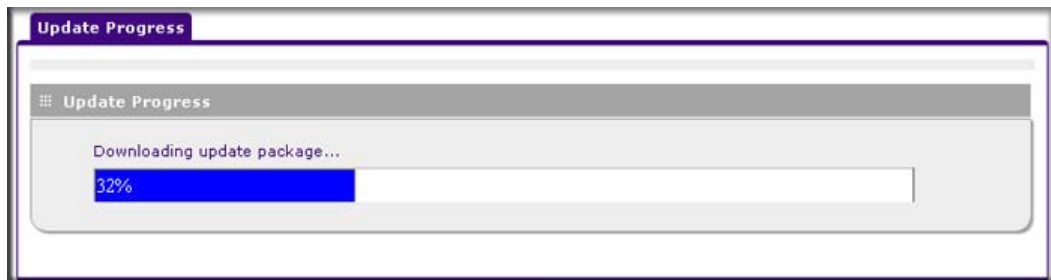


Figure 3-11

3. After the update has completed, click **Apply** to activate the newly updated software.

Critical Updates That Require a Restart

If a downloaded update requires a restart, you are prompted to perform the update when you log in to the STM. Figure 3-12 shows an example of a Critical Update screen, which provides information about the update and allows you to install it immediately or at a later time. To install the update immediately, click **Install Now**. To install the update at a later time, click **Later**.

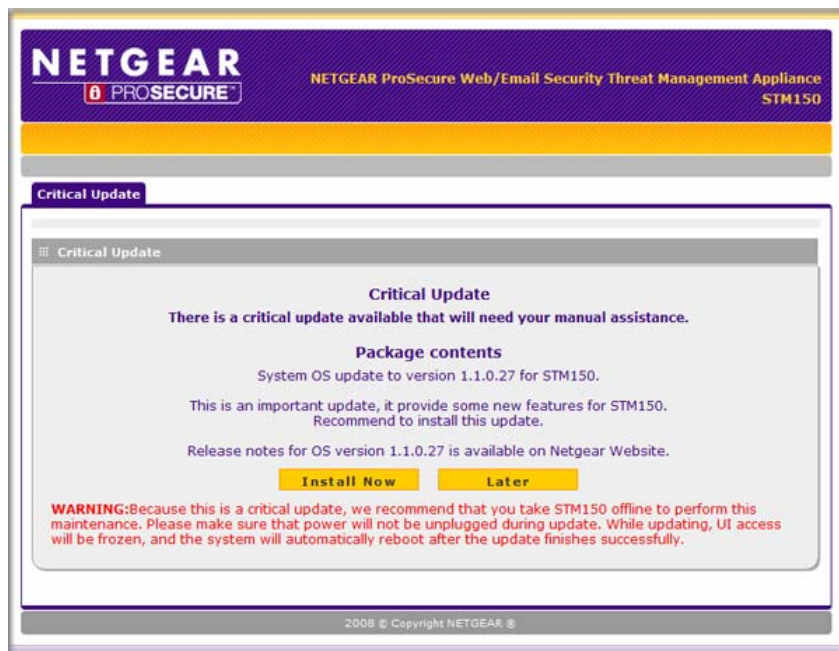


Figure 3-12

Configuring Date and Time Service

If you have used the Setup Wizard, you might have already configured the system date and time settings; the System Date and Time screen allows you to modify these settings.

Configure date, time and NTP server designations on the System Date and Time screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Setting the correct system time and time zone ensures that the date and time recorded in the STM logs and reports are accurate. Changing the time zone requires the STM to restart to apply the updated settings.

To set time, date and NTP servers:

1. Select **Administration > System Date and Time** from the menu. The System Date and Time screen displays.

The screenshot shows the 'System Date and Time' configuration page. At the top, there is a navigation bar with tabs for 'Global Settings', 'Email Security', 'Web Security', 'Application', 'Administration', 'User Management', 'Monitoring', and 'Support'. Below this is a sub-navigation bar with links for 'Remote Management', 'SNMP', 'Backup and Restore Settings', 'Software Update', 'Set Password', and 'System Date and Time'. The main content area is titled 'System Date and Time' and contains the following elements:

- Current Time:** 2009-08-02 00:19:30
- Use Default NTP Servers:** Selected (radio button).
- Use Custom NTP Servers:** Unselected (radio button).
 - Server 1 Name / IP Address: time-g.netgear.com
 - Server 2 Name / IP Address: time-h.netgear.com
- Manually Enter the Date and Time:** Unselected (radio button).
 - Date: [] - [] - [] (yyyy-mm-dd)
 - Time: [] : [] : [] (hh:mm:ss)
- Time Zone:** (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (pull-down menu).
- Note:** If applicable, daylight saving time will be applied automatically according to your selected time zone and city.
- Buttons:** Apply, Reset

Figure 3-13


The top of the screen displays the current weekday, date, time, time zone, and year (in the example in [Figure 3-13](#): Current Time: 2009-08-02 00:19:30).

2. Select the radio buttons, complete the fields, and make your selections from the pull-down menu as explained in [Table 3-8 on page 3-24](#).

Table 3-8. System Date and Time Settings

Setting	Description (or Subfield and Description)	
System Date and Time From the pull-down menu, select an NTP server, or select to enter the time manually.		
Use Default NTP Servers	The STM's real-time clock (RTC), which it uses for scheduling, is updated regularly by contacting a default NETGEAR NTP server on the Internet. This is the default setting.	
Use Custom NTP Servers	The STM's RTC is updated regularly by contacting one of the two NTP servers (primary and backup), both of which you must specify in the fields that become available with this menu selection. Note: If you select this option but leave either the Server 1 or Server 2 field blank, both fields are automatically set to the default NETGEAR NTP servers. Note: A list of public NTP servers is available at http://ntp.isc.org/bin/view/Servers/WebHome .	
	Server 1 Name / IP Address	Enter the IP address or host name the primary NTP server.
	Server 2 Name / IP Address	Enter the IP address or host name the secondary NTP server.
Manually Enter the Date and Time	Date	Enter the date in the yyyy-mm-dd (year-month-date) format.
	Time	Enter the time in the hh-mm-ss (hour-minutes-seconds) format.
Time Zone		
From the pull-down menu, select the local time zone in which the STM operates. The proper time zone is required in order for scheduling to work correctly. You do not need to configure daylight savings time, which is applied automatically when applicable. Greenwich Mean Time (GMT) is the default setting. Note: When you select a time zone that is not associated with a location such as "(GMT -08:00) GMT-8", daylight savings time is automatically disabled. When you select a time zone that <i>is</i> associated with a location such as "(GMT -08:00) Pacific Time (US & Canada)", daylight savings time is automatically enabled.		

- Click **Apply** to save your settings. Changing the time zone requires the STM to restart.

	Note: If you select the default NTP servers or if you enter a custom server FQDN, the STM determines the IP address of the NTP server by performing a DNS lookup. You must configure a DNS server address in the Network menu before the STM can perform this lookup.
---	--

Managing Digital Certificates

The STM uses digital certificates (also known as X509 certificates) for secure web access connections over HTTPS (that is, SSL VPN connections).

Digital certificates can be either self-signed or can be issued by certification authorities (CAs) such as an internal Windows server or an external organizations such as Verisign or Thawte. On the STM, the uploaded digital certificate is checked for validity and purpose. The digital certificate is accepted when it passes the validity test and the purpose matches its use.

The STM uses digital certificates to authenticate connecting HTTPS servers, and to allow HTTPS clients to be authenticated by remote entities. A digital certificate that authenticates a server, for example, is a file that contains the following elements:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified.

When a security alert is generated, the user can decide whether or not to trust the host.



Figure 3-14

You can obtain a digital certificate from a well-known commercial certificate authority (CA) such as Verisign or Thawte. Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server's identity.

The STM contains a self-signed digital certificate from NETGEAR. This certificate can be downloaded from the STM login screen or from the Certificate Management screen for browser

import. However, NETGEAR recommends that you replace this digital certificate with a digital certificate from a well-known commercial CA prior to deploying the STM in your network.

The STM's Certificate Management screen lets you to view the currently loaded digital certificate for HTTPS scans, upload a new digital certificate, manage the trusted CA authorities list, and manage the untrusted certificates list.

To display the Certificate Management screen, select **Web Security**> **Certificate Management** from the menu. Because of the size of this screen, and because of the way the information is presented, the Certificate Management screen is divided and presented in this manual in three figures ([Figure 3-15 on page 3-26](#), [Figure 3-16 on page 3-28](#), and [Figure 3-17 on page 3-29](#)).

Managing the Certificate for HTTPS Scans

To manage the STM's active certificate that is used for HTTPS scans:

Select **Web Security**> **Certificate Management** from the menu. The Certificate Management screen displays. [Figure 3-15](#) shows only the Certificate Used for HTTPS Scans section of the screen.

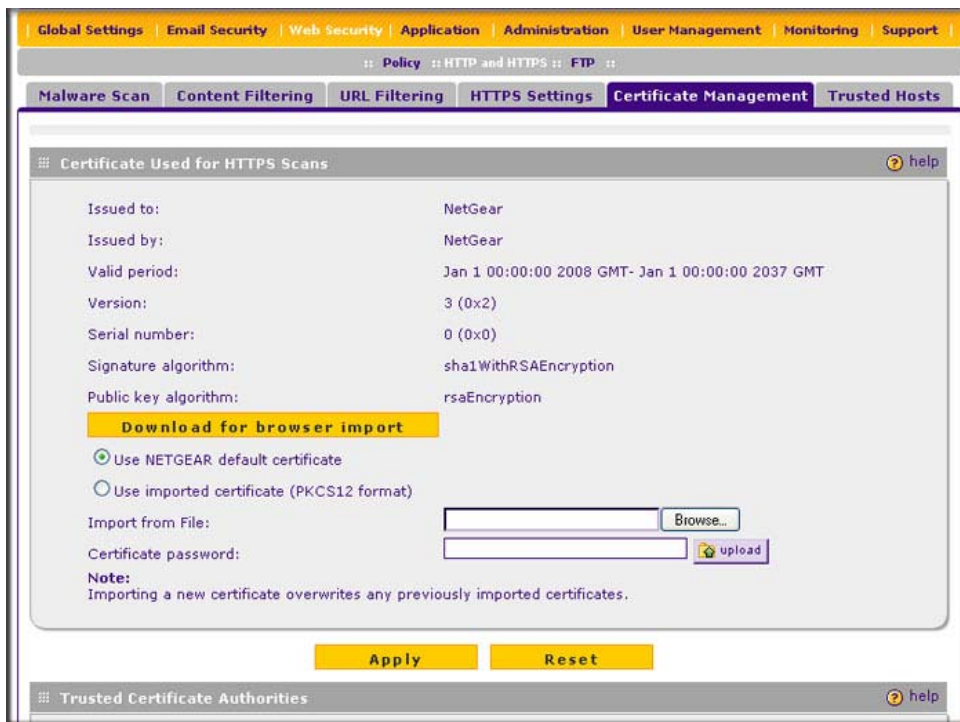


Figure 3-15

The top part of the Certificate Used for HTTPS Scans section displays information about the current certificate that is used for HTTPS scans



Note: For information about the HTTPS scanning process, “[HTTPS Scan Settings](#)” on page 4-36.

Downloading the Certificate in to Your Browser

To download the current certificate in to your browser:

1. Click **Download for browser Import**.
2. Follow the instructions of your browser to save the RootCA.crt file on your computer.

Reloading the Default NETGEAR Certificate

To reload the default NETGEAR certificate:

1. Select the **Use NETGEAR default certificate** radio button.
2. Click **Apply** to save your settings.

Importing a New Certificate

To import a new certificate:

1. Select the **Use imported certificate (PKCS12 format)** radio button.
2. Click **Browse** next to the Import from File field.
3. Navigate to a trusted certificate file on your computer. Follow the instructions of your browser to place the certificate file in the Import from File field.
4. If required, enter the appropriate password in the Certificate password field.
5. Click the **upload** button.



Note: If the certificate file is not in the pkcs12 format, the upload fails. Importing a new certificate overwrites any previously imported certificates.

6. Click **Apply** to save your settings.

Managing Trusted Certificates

To manage trusted certificates:

Select **Web Security > Certificate Management** from the menu. The Certificate Management screen displays. [Figure 3-16](#) shows only the Trusted Certificate Authorities section of the screen.



Figure 3-16

The Trusted Certificate Authorities table contains the trusted certificates from third-party Web sites that are signed by the Certificate Authorities.

Viewing Trusted Certificate Details

To view details of a trusted certificate:

1. Select the certificate from the Trusted Certificate Authorities table.
2. Click **View Details**. A new screen opens that displays the details of the certificate.

Deleting a Trusted Certificate

To delete a trusted certificate:

1. Select the certificate from the Trusted Certificate Authorities table.
2. Click **Delete Selected**.

Importing a Trusted Certificate

To import a trusted certificate:

1. Click **Browse** next to the Import from File field.
2. Navigate to a trusted certificate file on your computer. Follow the instructions of your browser to place the certificate file in the Import from File field.
3. Click the **upload** button. The newly imported trusted certificate is added to the Trusted Certificate Authorities table.

Managing Untrusted Certificates

To manage untrusted certificates:

Select **Web Security > Certificate Management** from the menu. The Certificate Management screen displays. [Figure 3-17](#) shows only the Untrusted Certificates section of the screen.



Figure 3-17

When the STM detects an untrusted or invalid certificate, it automatically places the certificate in the Untrusted Certificates table.

Viewing Untrusted Certificate Details

To view details of an untrusted certificate:

1. Select the certificate from the Untrusted Certificates table.
2. Click **View Details**. A new screen opens that displays the details of the certificate.

Deleting an Untrusted Certificate

To delete an untrusted certificate:

1. Select the certificate from the Untrusted Certificates table.
2. Click **Delete Selected**.

Moving an Untrusted Certificate to the Trusted Certificate Authorities Table

To move an untrusted certificate to the Trusted Certificate Authorities table:

1. Select the certificate from the Untrusted Certificates table.
2. Click **Add to Trusted List**. The previously untrusted certificate is added to the Trusted Certificate Authorities table.

Managing the Quarantine Settings

You can specify how much memory the STM reserves for quarantined items, and how long these items remain in memory. In general, the default settings work well for most situations.

To change the quarantine settings:

1. Select **Global Settings > Quarantine** from the menu. The Quarantine screen displays.

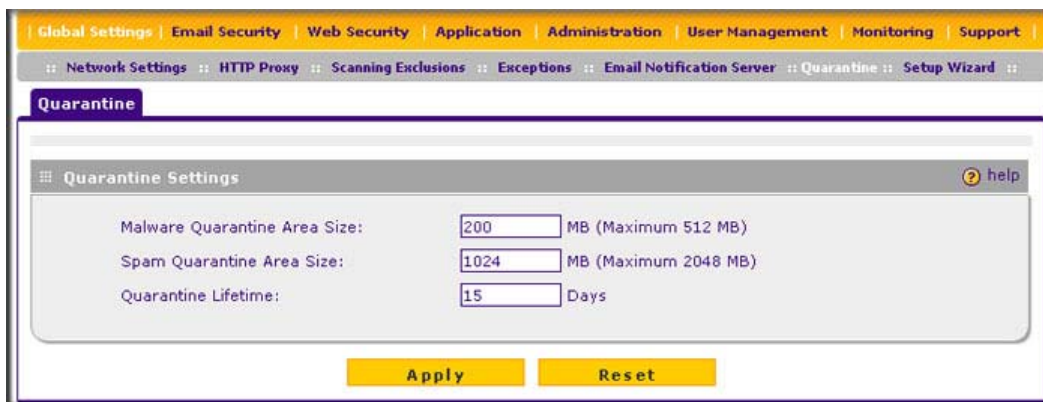


Figure 3-18

2. Select the radio buttons, complete the field, and make your selections from the pull-down menus as explained in [Table 3-9 on page 3-31](#).

Table 3-9. Quarantine Settings

Setting	Description (or Subfield and Description)
Malware Quarantine Area Size	Specify the maximum amount of memory in MB that is allocated to malware quarantine. This limit is commutative for all users. For the STM600, the default setting is 200 MB and the maximum setting is 512 MB. For the STM150 and STM300, the default setting is 100 MB and the maximum setting is 512 MB. Note: After the limit has been exceeded, old items are automatically purged from the malware quarantine to make space for new items.
Spam Quarantine Area Size	Specify the maximum amount of memory in MB that is allocated to spam quarantine. This limit is commutative for all users. For the STM600, the default setting is 1024 MB and the maximum setting is 2048 MB. For the STM150 and STM300, the default setting is 512 MB and the maximum setting is 1024 MB. Note: After the limit has been exceeded, old items are automatically purged from the malware quarantine to make space for new items.
Quarantine Lifetime	Specify how long items remain in quarantine before being automatically purged. The default setting is 15 days. The maximum setting is 30 days.

3. Click **Apply** to save your settings.



Note: To view and manage the quarantine files, see [“Viewing and Managing the Quarantine Files”](#) on page 6-33.

Performance Management

Performance management consists of controlling the traffic through the STM so that the necessary traffic gets through when there is a bottleneck and either reducing unnecessary traffic or rescheduling some traffic to low-peak times to prevent bottlenecks from occurring in the first place.

You can adjust the following features of the STM in such a way that the traffic load on the WAN side decreases

If you want to reduce traffic by preventing undesired e-mails from reaching their destinations or by preventing access to certain sites on the Internet, you can use the STM's content filtering feature. By default, this feature is disabled; all requested traffic from any Web site is allowed with the exception of Web content categories that are mentioned in [“Default E-mail and Web Scan Settings” on page 4-2](#).

- **E-mail Content Filtering.** To reduce incoming e-mail traffic, you can block e-mails with large attachments, reject e-mails based on keywords, file extensions, or file names, and set spam protection rules. There are several ways you can reduce undesired e-mail traffic:
 - **Setting the size of e-mail files to be scanned.** Scanning large e-mail files requires network resources and might slow down traffic. You can specify the maximum file or message size that is scanned, and if files that exceed the maximum size are skipped (which might compromise security) or blocked. For more information, see [“Configuring E-mail Anti-Virus Exception Settings” on page 4-7](#).
 - **Keyword, file extension, and file name blocking.** You can reject e-mails based on keywords in the subject line, file type of the attachment, and file name of the attachment. For more information, see [“E-mail Content Filtering” on page 4-11](#).
 - **Protecting against spam.** Set up spam protection to prevent spam from using up valuable bandwidth. For more information, see [“Protecting Against E-mail Spam” on page 4-14](#).
- **Web Content Filtering.** The STM provides extensive methods to filtering Web content in order to reduce traffic:
 - **Web category blocking.** You can block entire Web categories because their content is undesired, offensive, or not relevant, or simply to reduce traffic. For more information, see [“Configuring Web Content Filtering” on page 4-26](#).
 - **File extension blocking.** You can block files based on their extension. Such files can include, executable files, audio and video files, and compressed files. For more information, see [“Configuring Web Content Filtering” on page 4-26](#).
 - **URL blocking.** You can specify URLs that are blocked by the STM. For more information, see [“Configuring Web URL Filtering” on page 4-32](#).
 - **Web services blocking.** You can block Web applications such as instant messaging, media, peer-to-peer, and tools. For more information, see [“Configuring Application Control” on page 4-44](#).
 - **Web object blocking.** You can block the following Web component types: embedded objects (ActiveX, Java, Flash), proxies, and cookies, and you can disable Java scripts. For more information, see [“Configuring Web Content Filtering” on page 4-26](#).

- **Setting the size of Web files to be scanned.** Scanning large Web files requires network resources and might slow down traffic. You can specify the maximum file size that is scanned, and if files that exceed the maximum size are skipped (which might compromise security) or blocked. For more information, see [“Configuring Web Malware Scans” on page 4-24](#).

For these features (with the exception of Web object blocking and setting the size of files to be scanned), you can set schedules to specify when Web content is filtered (see [“Configuring Web Content Filtering” on page 4-26](#)) and configure scanning exclusions and access exceptions (see [“Setting Scanning Exclusions and Web Access Exceptions” on page 4-46](#)).

You can use the STM’s monitoring functions to assist you with performance management (see [“Monitoring Real-Time Traffic, Security, Statistics, and Web Usage” on page 6-11](#)).

Chapter 4

Content Filtering and Optimizing Scans

This chapter describes how to apply the content filtering features of the STM and how to optimize scans to protect your network. This chapter contains the following sections:

- [“About Content Filtering and Scans”](#) on this page.
- [“Configuring E-mail Protection”](#) on page 4-4.
- [“Configuring Web and Services Protection”](#) on page 4-22.
- [“Configuring Application Control”](#) on page 4-44.
- [“Setting Scanning Exclusions and Web Access Exceptions”](#) on page 4-46.

About Content Filtering and Scans

The STM provides very extensive Web content and e-mail content filtering options, Web browsing activity reporting, e-mail anti-virus and anti-spam options, and instant alerts via e-mail. You can establish restricted Web access policies that are based on the time-of-day, Web addresses, and Web address keywords. You can also block Internet access by applications and services, such as instant messaging and peer to peer file sharing clients.



Note: For information about how to monitor blocked content and malware threats in real-time, see [“Monitoring Real-Time Traffic, Security, Statistics, and Web Usage”](#) on page 6-11. For information about how to view blocked content and malware threats in the logs, see [“Querying the Logs”](#) on page 6-22. For information about how to view quarantined content, see [“Viewing and Managing the Quarantine Files”](#) on page 6-33.

Default E-mail and Web Scan Settings

For most network environments, the default scan settings and actions that are shown in [Table 4-1](#) work well but you can adjust these to the needs of your specific environment.

Table 4-1. Default E-mail and Web Scan Settings

Scan Type	Default Scan Setting	Default Action (if applicable)
Email Server Protocols		
SMTP	Enabled	Block infected e-mail
POP3	Enabled	Delete attachment if infected
IMAP	Enabled	Delete attachment if infected
Web Server Protocols ^a		
HTTP	Enabled	Delete file if malware threat detected
HTTPS	Disabled	No action (scan disabled)
FTP	Enabled	Delete file if malware threat detected
Instant Messaging Services		
Google Talk	Allowed	
ICQ	Allowed	
mIRC	Allowed	
MSN Messenger	Allowed	
QQ	Allowed	
Yahoo Messenger	Allowed	
Media Applications		
iTunes (music store, update)	Allowed	
Quicktime (update)	Allowed	
Real Player (guide)	Allowed	
Rhapsody (guide, music store)	Allowed	
Winamp (Internet radio/TV)	Allowed	
Peer-to-Peer (P2P) Services		
BitTorrent	Allowed	
eDonkey	Allowed	
Gnutella	Allowed	

Table 4-1. Default E-mail and Web Scan Settings (continued)

Scan Type	Default Scan Setting	Default Action (if applicable)
Tools		
Alexa Toolbar	Allowed	
GoToMyPC	Allowed	
Weatherbug	Allowed	
Yahoo Toolbar	Allowed	
Web Objects		
Embedded Objects (ActiveX/Java/Flash)	Allowed	
Javascript	Allowed	
Proxy	Allowed	
Cookies	Allowed	
Web Content Categories		
Commerce	Allowed	
Drugs and Violence	Blocked	
Education	Allowed with the exception of School Cheating.	
Gaming	Blocked	
Inactive Sites	Allowed	
Internet Communication and Search	Allowed with the exception of Anonymizers	
Leisure and News	Allowed	
Malicious	Blocked	
Politics and Religion	Allowed	
Sexual Content	Blocked	
Technology	Allowed	
Uncategorized	Blocked	

a. For the STM300 and STM600, files and messages that are larger than 10240 KB are skipped by default. For the STM150, files and messages that are larger than 8192 KB are skipped by default.

Configuring E-mail Protection

The STM lets you configure the following settings to protect the network's e-mail communication:

- The e-mail protocols that are scanned for malware threats.
- Actions that are taken when infected e-mails are detected.
- The maximum file sizes that are scanned.
- Keywords, file types, and file names in e-mails that are filtered to block objectionable or high-risk content.
- Customer notifications and e-mail alerts that are sent when events are detected.
- Rules and policies for spam detection.

Customizing E-mail Protocol Scan Settings

If you have used the Setup Wizard, you might have already configured the e-mail policies; the (e-mail) Policy screen allows you to modify these settings.

To configure the e-mail protocols and ports to scan:

1. Select **Email Security > Policy** from the menu. The (e-mail) Policy screen displays.

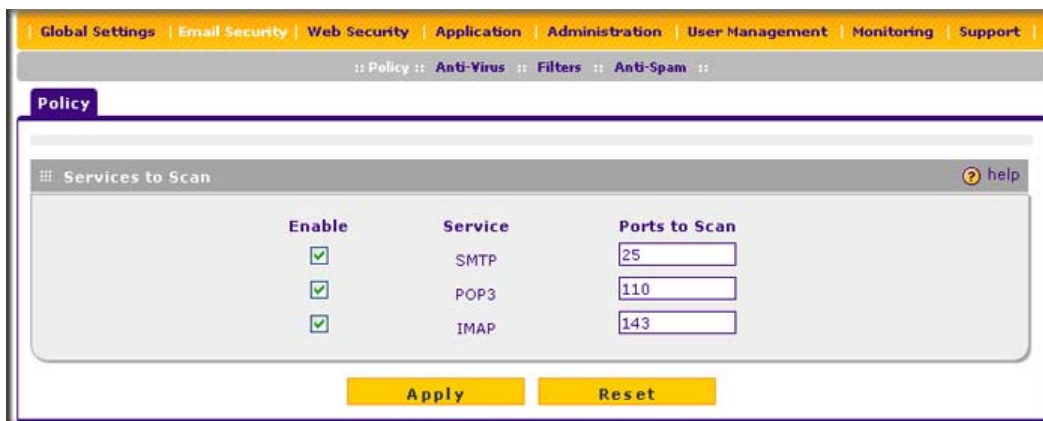




Figure 4-1

- Complete the fields and select the checkboxes as explained in [Table 4-2](#).

Table 4-2. E-mail Policy Settings

Setting	Description
Services to Scan	
SMTP	Select the SMTP checkbox to enable Simple Mail Transfer Protocol (SMTP) scanning. This service is enabled by default and uses default port 25.
POP3	Select the POP3 checkbox to enable Post Office Protocol 3 (POP3). This service is enabled by default and uses default port 110.
IMAP	Select the IMAP checkbox to enable Internet Message Access Protocol (IMAP). This service is enabled by default and uses default port 143.

	Note: If a protocol uses a port other than the standard service port (for example, port 25 for SMTP), enter this non-standard port in the Ports to Scan field. For example, if the SMTP service on your network uses both port 25 and port 2525, enter both port numbers in the Ports to Scan field and separate them by a comma.
---	--

	Note: The following protocols are not supported by the STM: SMTP over SSL using port number 465, POP3 over SSL using port number 995, and IMAP over SSL using port number 993.
---	---

- Click **Apply** to save your settings.

Customizing E-mail Anti-Virus Settings

If you have used the Setup Wizard, you might have already configured the e-mail anti-virus action and exception settings; the Action and Exception screens allows you to modify these settings. The Notification screen allows you to specify the e-mail anti-virus notification settings.

Whether or not the STM detects an e-mail virus, you can configure it to take a variety of actions (some of the default actions are listed in [Table 4-1 on page 4-2](#)), set exceptions for file sizes, and specify which notifications, e-mails, or both must be sent to the end users.

Configuring E-mail Anti-Virus Action Settings

To configure the e-mail anti-virus action settings:

- Select **Email Security > Anti-Virus** from the menu. The anti-virus submenu tabs appear with the Action screen in view (see [Figure 4-2 on page 4-6](#)).

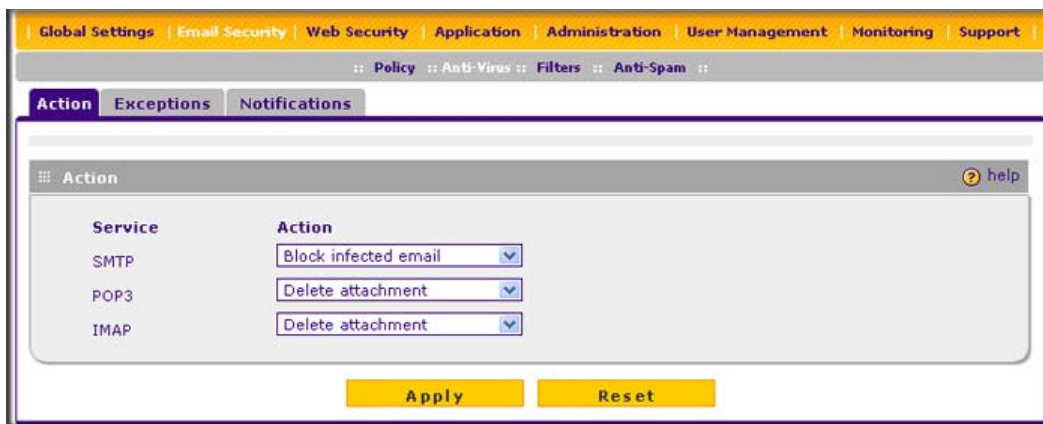


Figure 4-2

- Complete the fields, select the checkboxes, and make your selections from the pull-down menus as explained in [Table 4-3](#).

Table 4-3. E-mail Anti-Virus Action Settings

Setting	Description
Action	
SMTP	<p>From the SMTP pull-down menu, specify one of the following actions when an infected e-mail is detected:</p> <ul style="list-style-type: none"> • Quarantine attachment. The e-mail is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Delete attachment. The e-mail is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created. • Block infected email. This is the default setting. The e-mail is blocked, and a virus log entry or a spyware log entry is created. • Quarantine infected email. The e-mail is placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Log only. Only a virus log entry or a spyware log entry is created. The e-mail is not blocked and the attachment is not deleted.

Table 4-3. E-mail Anti-Virus Action Settings (continued)

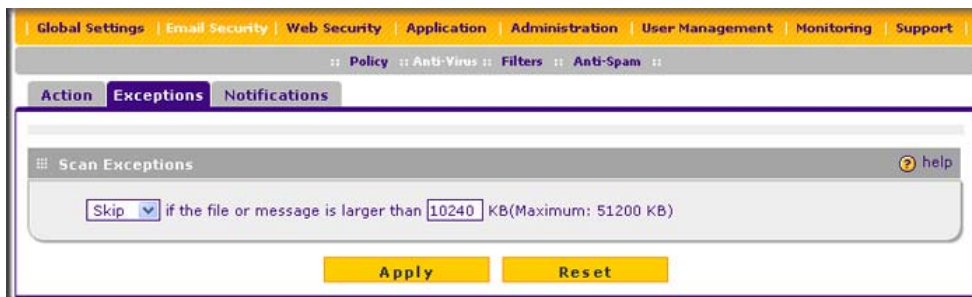
Setting	Description
POP3	<p>From the POP3 pull-down menu, specify one of the following actions when an infected e-mail is detected:</p> <ul style="list-style-type: none"> • Quarantine attachment. The e-mail is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Delete attachment. This is the default setting. The e-mail is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created. • Log only. Only a virus log entry or a spyware log entry is created. The e-mail is not blocked and the attachment is not deleted.
IMAP	<p>From the IMAP pull-down menu, specify one of the following actions when an infected e-mail is detected:</p> <ul style="list-style-type: none"> • Quarantine attachment. The e-mail is not blocked, but the attachment is removed and placed in the malware quarantine for further research. In addition, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Delete attachment. This is the default setting. The e-mail is not blocked, but the attachment is deleted, and a virus log entry or a spyware log entry is created. • Log only. Only a virus log entry or a spyware log entry is created. The e-mail is not blocked and the attachment is not deleted.

3. Click **Apply** to save your settings.

Configuring E-mail Anti-Virus Exception Settings

To configure the e-mail anti-virus exception settings:

1. Select **Email Security > Anti-Virus** from the menu. The anti-virus submenu tabs appear with the Action screen in view.
2. Click the **Exceptions** submenu tab. The Exceptions screen displays.

**Figure 4-3**

3. Make your selection from the pull-down menus and complete the field as explained in [Table 4-4](#).

Table 4-4. E-mail Anti-Virus Exception Settings

Setting	Description
Scan Exceptions	
<p>From the pull-down menu, specify one of the following actions when an e-mail attachment exceeds the size that you specify in the file size field:</p> <ul style="list-style-type: none"> • Skip. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • Block. The file is blocked and does not reach the end user. <p>The default and maximum file sizes are:</p> <ul style="list-style-type: none"> • For the STM600 and STM300, the default setting is to block any attachment larger than 10240 KB. The maximum file size that you can specify is 51200 KB. • For the STM150, the default setting is to block any attachment larger than 8192 KB. The maximum file size that you can specify is 25600 KB. 	



Note: Setting the maximum file size to a high value might affect the STM's performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats.

4. Click **Apply** to save your settings.

Configuring E-mail Anti-Virus Notification Settings

To configure the e-mail anti-virus notification settings:

1. Select **Email Security > Anti-Virus** from the menu. The anti-virus submenu tabs appear with the Action screen in view.
2. Click the **Notifications** submenu tab. The Notifications screen displays (see [Figure 4-4 on page 4-9](#)).

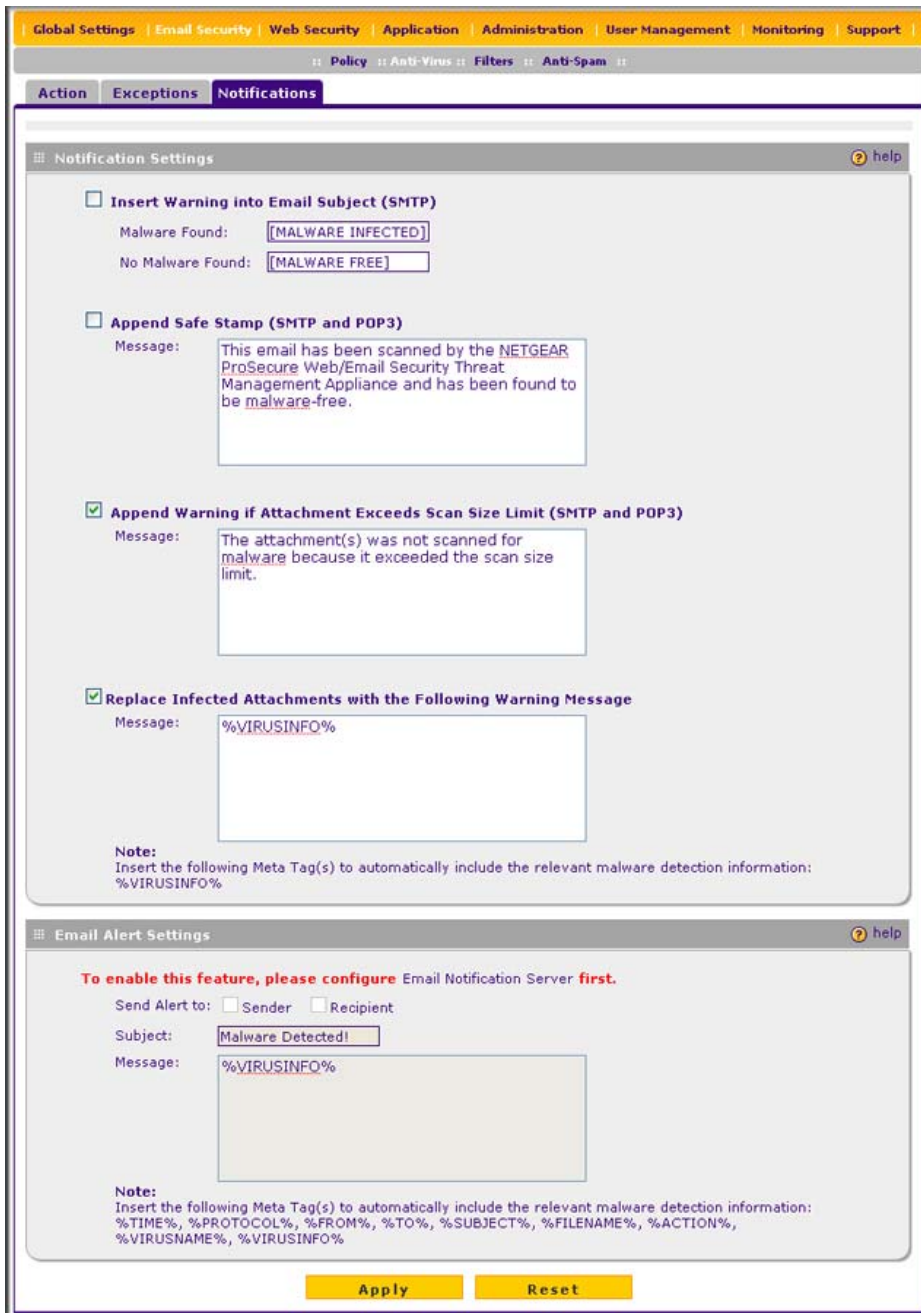


Figure 4-4

3. Complete the fields, select the checkboxes, and make your selections from the pull-down menus as explained in [Table 4-5](#).

Table 4-5. E-mail Anti-Virus Notification Settings

Setting	Description
Notification Settings	
Insert Warning into Email Subject (SMTP)	For SMTP e-mail messages, select this checkbox to insert a warning into the e-mail subject line: <ul style="list-style-type: none"> • Malware Found. If a malware threat is found, a “[MALWARE INFECTED]” message is inserted. You can change this default message. • No Malware Found. If no malware threat is found, a “[MALWARE FREE]” message is inserted. You can change this default message. By default, this checkbox is deselected and no warnings are inserted.
Append Safe Stamp (SMTP and POP3)	For SMTP and POP3 e-mail messages, select this checkbox to insert a default safe stamp message at the end of an e-mail. The safe stamp insertion serves as a security confirmation to the end user. You can change the default message. By default, this checkbox is deselected and no safe stamp is inserted.
Append Warning if Attachment Exceeds Scan Size Limit (SMTP and POP3)	For SMTP and POP3 e-mail messages, select this checkbox to append a default warning message to an e-mail if the message or an attachment to the message exceeds the scan size limit. The warning message informs the end user that the attachment was skipped and might not be safe to open. You can change the default message. By default, this checkbox is selected and a warning message is appended to the e-mail.
Replace Infected Attachments with the Following Warning Message	Select this checkbox to replace an e-mail that is infected with a default warning message. The warning message informs the end user about the name of the malware threat. You can change the default message to include the action that the STM has taken (see example below). By default, this checkbox is selected and a warning message replaces an infected e-mail. <p>Note: Make sure that you keep the %VIRUSINFO% meta word in a message to enable the STM to insert the proper malware threat information. The following is an example message where the %VIRUSINFO% meta word is replaced with the EICAR test virus:</p> <p>“This attachment contains malware: File 1.exe contains malware EICAR. Action: Delete.”</p>

Table 4-5. E-mail Anti-Virus Notification Settings (continued)

Setting	Description
Email Alert Settings Note: Ensure that the E-mail Notification Server (see “Configuring the E-mail Notification Server” on page 6-2) is configured before you specify the e-mail alert settings.	
Send alert to	In addition to inserting an warning message to replace an infected e-mail, you can configure the STM to send a notification e-mail to the sender, the recipient, or both by selecting the corresponding checkbox or checkboxes. By default, both checkboxes are deselected and no notification e-mail is sent.
Subject	The default subject line for the notification e-mail is “Malware detected!” You can change this subject line.
Message	The warning message informs the sender, the recipient, or both about the name of the malware threat. You can change the default message to include more information. Note: Make sure that you keep the %VIRUSINFO% meta word in a message to enable the STM to insert the proper malware threat information. In addition to the %VIRUSINFO% meta word, you can insert the following meta words in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.

4. Click **Apply** to save your settings.

E-mail Content Filtering

The STM provides several options to filter unwanted content from e-mails. You can filter content from e-mails based on keywords in the subject line, file type of the attachment, and file name of the attachment. You can also set an action to perform on e-mails with password-protected attachments.

Several types of e-mail blocking are available:

- **Keyword blocking.** You can specify words that, should they appear in the e-mail subject line, cause that e-mail to be blocked by the STM.
- **Password-protected attachments.** You can block e-mails based on password-protected attachments such as ZIP or RAR attachments.
- **File extension blocking.** You can block e-mails based on the extensions of attached files. Such files can include, executable files, audio and video files, and compressed files.
- **File name blocking.** You can block e-mails based on the names of attached files. Such names can include, for example, names of known malware threats such as the Netsky worm (which normally arrives as netsky.exe).

To configure e-mail content filtering:

1. Select **Email Security > Filters** from the menu. The Filters screen displays.

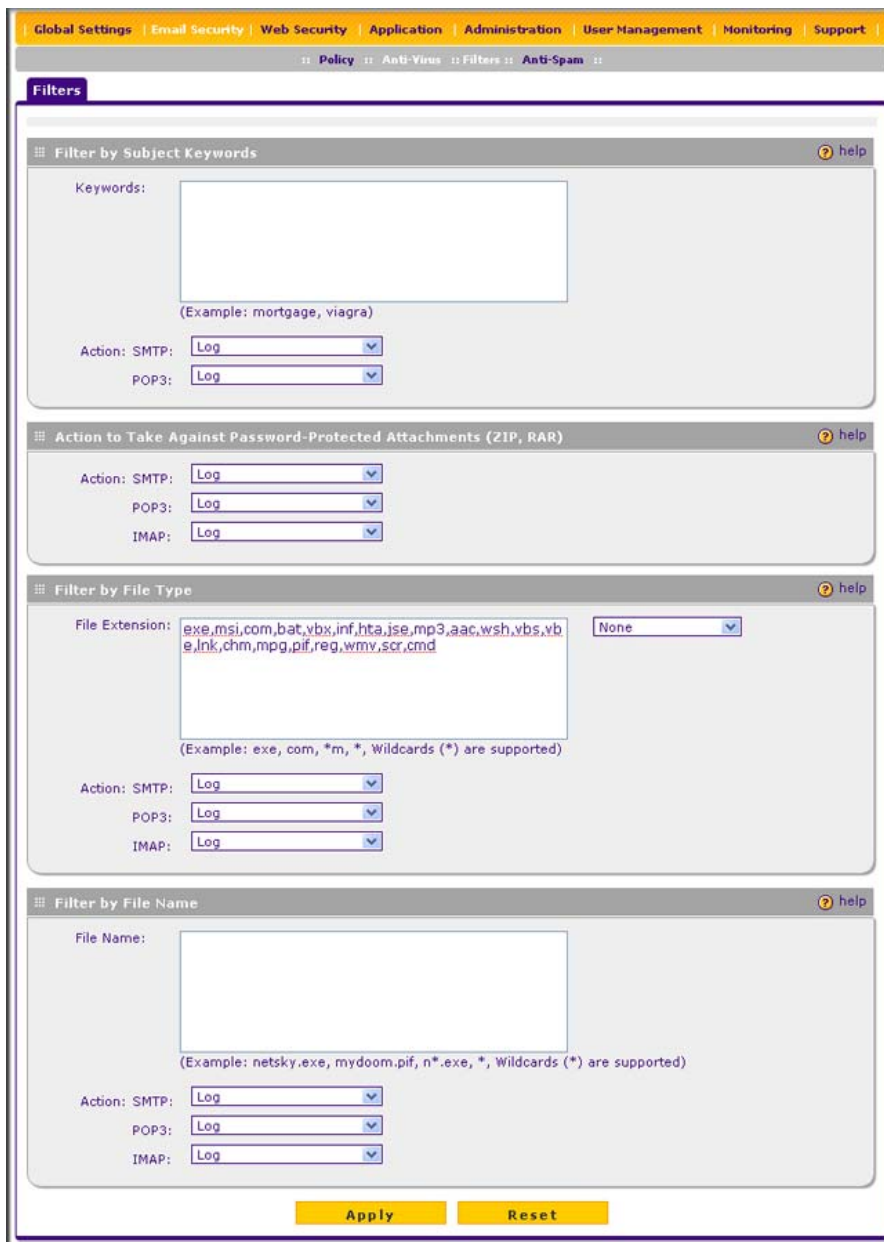


Figure 4-5

2. Complete the fields and make your selections from the pull-down menus as explained in [Table 4-6](#).

Table 4-6. E-mail Filter Settings

Setting	Description (or Subfield and Description)	
Filter by Subject Keywords		
Keywords	Enter keywords that are detected in the e-mail subject line. Use commas to separate different keywords. The total maximum length of this field is 2048 characters, excluding duplicate words and delimiter commas.	
Action	SMTP	From the SMTP pull-down menu, specify one of the following actions when a keyword that is defined in the Keywords field is detected: <ul style="list-style-type: none"> • Block email & Log. The e-mail is blocked, and a log entry is created. • Log. This is the default setting. Only a log entry is created. The e-mail is not blocked.
	POP3	From the POP3 pull-down menu, specify one of the following actions when a keyword that is defined in the Keywords field is detected: <ul style="list-style-type: none"> • Block email & Log. The e-mail is blocked, and a log entry is created. • Log. This is the default setting. Only a log entry is created. The e-mail is not blocked.
Filter by Password-Protected Attachments (ZIP, RAR, etc.)		
Action	SMTP	From the SMTP pull-down menu, specify one of the following actions when a password-protected attachment to an e-mail is detected: <ul style="list-style-type: none"> • Block attachment & Log. The e-mail is not blocked, the attachment is blocked, and a log entry is created. • Block email & Log. The e-mail is blocked, and a log entry is created. • Log. This is the default setting. Only a log entry is created. The e-mail and attachment are not blocked.
	POP3	From the POP3 pull-down menu, specify one of the following actions when a password-protected attachment to an e-mail is detected: <ul style="list-style-type: none"> • Block attachment & Log. The e-mail is not blocked, the attachment is blocked, and a log entry is created. • Log. This is the default setting. Only a log entry is created. The e-mail and attachment are not blocked.
	IMAP	From the IMAP pull-down menu, specify one of the following actions when a password-protected attachment to an e-mail is detected: <ul style="list-style-type: none"> • Block attachment & Log. The e-mail is not blocked, the attachment is blocked, and a log entry is created. • Log. This is the default setting. Only a log entry is created. The e-mail and attachment are not blocked.

Table 4-6. E-mail Filter Settings (continued)

Setting	Description (or Subfield and Description)	
Filter by File Type		
File Extension	<p>By default, the File Extension field lists the most common file extensions that are detected. You can manually add or delete extensions. Use commas to separate different extensions. You can enter a maximum of 40 file extensions; the maximum total length of this field, excluding the delimiter commas, is 160 characters.</p> <p>You can also use the pull-down menu to add predefined file extensions from a specific category to the File Extension field:</p> <ul style="list-style-type: none"> • None. No file extensions are added to the File Extension field. This is the default setting. • Executables. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field. • Audio/Video. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field. • Compressed Files. Compressed file extensions (zip, rar, gz, tar, and bz2) added to the File Extension field. 	
Action	SMTP	From the pull-down menu, specify an action when an e-mail attachment with a file extension that is defined in the File Extension field is detected. The pull-down menu selections and defaults are the same as the ones for the “Filter by Password-Protected Attachments (ZIP, RAR, etc.)” section above.
	POP3	
	IMAP	
Filter by File Name		
File Name	Enter the file names that are detected. For example, to block the Netsky worm (which normally arrives as netsky.exe), enter netsky.exe. You can enter a maximum of 20 file names. Use commas to separate multiple file names. The maximum total length of this field is 400 characters, excluding the delimiter commas.	
Action	SMTP	From the pull-down menu, specify an action when an e-mail attachment with a name that is defined in the File Name field is detected. The pull-down menu selections and defaults are the same as the ones for the “Filter by Password-Protected Attachments (ZIP, RAR, etc.)” section above.
	POP3	
	IMAP	

3. Click **Apply** to save your settings.

Protecting Against E-mail Spam

The STM integrates multiple anti-spam technologies to provide comprehensive protection against unwanted e-mail. You can enable all or a combination of these anti-spam technologies.

The STM implements these spam prevention technologies in the following order:

1. **Whitelist.** E-mails from the specified sources or to the specified recipients are not considered spam and are accepted.

2. **Blacklist.** E-mails from the specified sources are considered spam and are blocked.
3. **Real-time blacklist.** E-mails from known spam sources that are collected by blacklist providers are blocked.
4. **Distributed spam analysis.** E-mails that are detected as spam by the NETGEAR Spam Classification Center are either tagged, blocked, or quarantined.

This order of implementation ensures the optimum balance between spam prevention and system performance. For example, if an e-mail originates from a whitelisted source, the STM delivers the e-mail immediately to its destination inbox without implementing the other spam prevention technologies, thereby speeding up mail delivery and conserving the STM system resources. However, regardless of whether or not an e-mail is whitelisted, it still be scanned by the STM's anti-malware engines.

You can configure these anti-spam options in conjunction with content filtering to optimize blocking of unwanted mails.



Note: E-mails that are sent through the STM over an authenticated connection between a client and an SMTP mail server are not checked for spam.



Note: An e-mail that has been checked for spam by the STM contains an “X-STM-SMTP” (for SMTP e-mails) or “X-STM-POP3” (for POP-3 e-mails) tag in its header.

Setting Up the Whitelist and Blacklist

You can specify e-mails that are accepted or blocked based on the originating IP address, domain, and e-mail address by setting up the whitelist and blacklist. You can also specify e-mails that are accepted based on the destination domain and e-mail address.

The whitelist ensures that e-mail from listed (that is, trusted) sources and recipients are not mistakenly tagged as spam. E-mails going to and from these sources and recipients are delivered to their destinations immediately, without being scanned by the anti-spam engines. This can help to speed up the system and network performance. The blacklist, on the other hand, lists sources from which all e-mail messages are blocked. You can enter up to 200 entries per list, separated by commas.



Note: The whitelist takes precedence over the blacklist, which means that if an e-mail source is on both the blacklist and the whitelist, the e-mail is not scanned by the anti-spam engines.

To configure the whitelist and blacklist:

1. Select **Email Security > Anti-Spam** from the menu. The Anti-Spam submenu tabs appear, with the Whitelist/Blacklist screen in view.

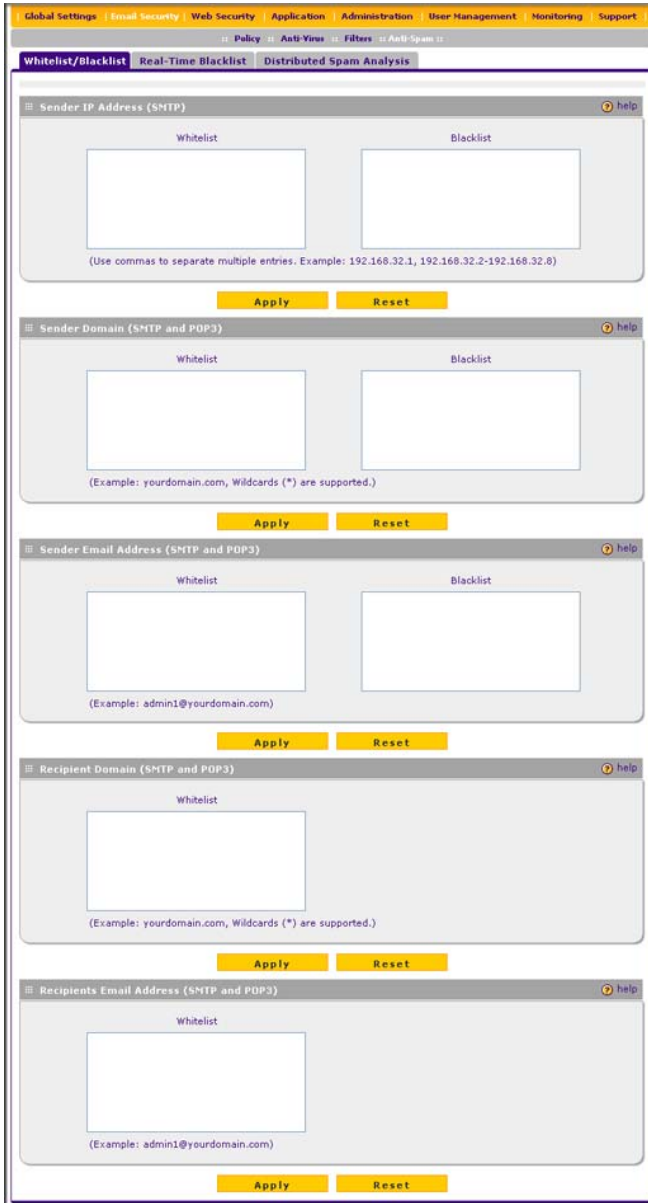



Figure 4-6

2. Complete the fields as explained in [Table 4-6](#).

Table 4-7. Whitelist/Blacklist Settings

Setting	Description
Sender IP Address (SMTP)	
Whitelist	Enter the source IP addresses from which e-mails can be trusted.
Blacklist	Enter the source IP addresses from which e-mails are blocked.
Click Apply to save your settings or click Reset to clear all entries from these fields.	
Sender Domain (SMTP and POP3)	
Whitelist	Enter the sender e-mail domains from which e-mails can be trusted.
Blacklist	Enter the sender e-mail domains from which e-mails are blocked.
Click Apply to save your settings or click Reset to clear all entries from these fields.	
Sender Email Address (SMTP and POP3)	
Whitelist	Enter the e-mail addresses from which e-mails can be trusted.
Blacklist	Enter the e-mail addresses from which e-mails are blocked.
Click Apply to save your settings or click Reset to clear all entries from these fields.	
Recipients Domain (SMTP and POP3)	
Whitelist	Enter the e-mail domains of the recipients to which e-mails can be safely delivered.
Click Apply to save your settings or click Reset to clear all entries from this field.	
Recipients Email Address (SMTP and POP3)	
Whitelist	Enter the e-mail addresses of the recipients to which e-mails can be safely delivered.
Click Apply to save your settings or click Reset to clear all entries from this field.	

	Note: In the fields of the Whitelist/Blacklist screen, use commas to separate multiple entries. For IP addresses, use a dash to indicate a range (for example, 192.168.32.2-192.168.32.8.)
---	---

Configuring the Real-time Blacklist

Blacklist providers are organizations that collect IP addresses of verified open SMTP relays that might be used by spammers as media for sending spam. These known spam relays are compiled by blacklist providers and are made available to the public in the form of real-time blacklists (RBLs). By accessing these RBLs, the STM can block spam originating from known spam sources.

By default, the STM comes with two pre-defined blacklist providers: Spamhaus, and Spamcop. You can add a maximum of 16 blacklist providers to the RBL sources.

To enable the real-time blacklist:

1. Select **Email Security > Anti-Spam** from the menu. The Anti-Spam submenu tabs appear, with the Whitelist/Blacklist screen in view.
2. Click the **Real-time Blacklist** submenu tab. The Real-time Blacklist screen displays.

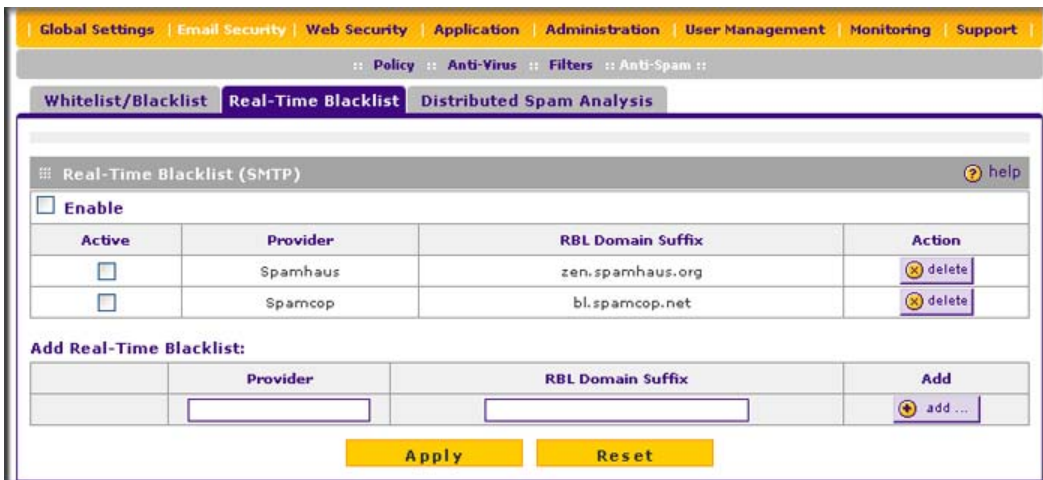


Figure 4-7

3. Select the **Enable** checkbox enable the Real-Time Blacklist function.
4. Select the **Active** checkboxes to the left of the default blacklist providers (Spamhaus and Spamcop) that you want to activate.
5. Click **Apply** to save your settings.

To add a blacklist provider to the real-time blacklist:

1. In the Add Real-time Blacklist section, add the following information:
 - In the Provider field, add the name of the blacklist provider.
 - In the RBL Domain Suffix field, enter the domain suffix of the blacklist provider.
2. Click the **add** table button in the Add column. The new blacklist provider is added to the Real-time Blacklist (SMTP) table, and it is disabled by default.

To delete a blacklist provider from the real-time blacklist, click the **delete** table button next to the blacklist provider that you want to delete.

Configuring Distributed Spam Analysis

Spam, phishing, and other e-mail-borne threats consist of millions of messages intentionally composed differently to evade commonly-used filters. Nonetheless, all messages within the same outbreak share at least one unique, identifiable value which can be used to distinguish the outbreak.

With distributed spam analysis, message patterns are extracted from the message envelope, headers, and body with no reference to the content, itself. Pattern analysis can then be applied to identify outbreaks in any language, message format, or encoding type. Message patterns can be divided into distribution patterns and structure patterns. Distribution patterns determine if the message is legitimate or a potential threat by analyzing the way it is distributed to the recipients, while structure patterns determine the volume of the distribution.

The STM uses a Distributed Spam Analysis architecture to determine whether or not an e-mail is spam for SMTP and POP3 e-mails. Any e-mail that is identified as spam is tagged as spam (an option for both SMTP and POP3), blocked, or quarantined (the latter two are options possible only for SMTP).



Note: Unlike other scans, you do not need to configure the spam score because the NETGEAR Spam Classification Center performs the scoring automatically as long as the STM is connected to the Internet. However, this does mean that the STM must be connected to the Internet for the spam analysis to be performed correctly.

To configure Distributed Spam Analysis and the anti-spam engine settings:

1. Select **Email Security > Anti-Spam** from the menu. The Anti-Spam submenu tabs appear, with the Whitelist/Blacklist screen in view.
2. Click the **Distributed Spam Analysis** submenu tab. The Distributed Spam Analysis screen displays (see [Figure 4-8 on page 4-20](#)).

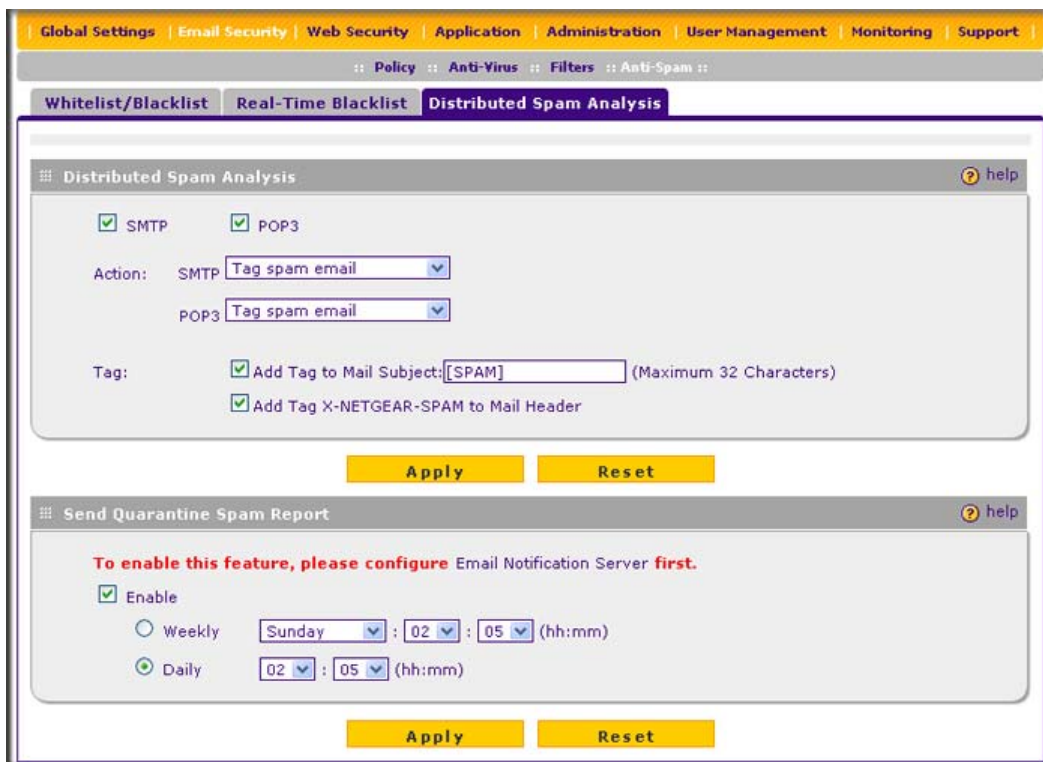


Figure 4-8

3. Complete the fields, select the checkboxes, and make your selections from the pull-down menus as explained in Table 4-8.

Table 4-8. Distributed Spam Analysis Settings

Setting	Description (or Subfield and Description)
Distributed Spam Analysis	
SMTP	Select the SMTP checkbox to enable Distributed Spam Analysis for the SMTP protocol. (You can enable Distributed Spam Analysis for both SMTP and POP3.)
POP3	Select the POP3 checkbox to enable Distributed Spam Analysis for the POP3 protocol. (You can enable Distributed Spam Analysis for both SMTP and POP3.)

Table 4-8. Distributed Spam Analysis Settings (continued)

Setting	Description (or Subfield and Description)	
Action	SMTP	From the SMTP pull-down menu, select the action that are taken when spam is detected by the anti-spam engine: <ul style="list-style-type: none"> • Tag spam email. This is the default setting. The e-mail is tagged as spam, and a spam log entry is created. • Block spam email. The e-mail is blocked, and a spam log entry is created. • Quarantine spam email. The e-mail is quarantined, a spam log entry is created, and a spam quarantine log entry is created.
	POP3	The only option is to tag spam e-mail. A spam log entry is also created.
Tag	Add tag to mail subject	When the option "Tag spam email" is selected from the Action pull-down menu (see above), select this checkbox to add a tag to the e-mail subject line. The default tag is "[SPAM]" but you can customize this tag. The default setting is to add the default tag to the subject line.
	Add tag X-NETGEAR-SPAM to mail header	When the option "Tag spam email" is selected from the Action pull-down menu (see above), select this checkbox to add the "X-NETGEAR-SPAM" tag to the e-mail header. The default setting is to add the default tag to the e-mail header.
Send Quarantine Spam Report Note: Ensure that the Email Notification Server (see "Configuring the E-mail Notification Server" on page 6-2) is configured before you specify the quarantine spam report settings.		
Enable	Select this checkbox to enable the STM to send a quarantine spam report to the recipient that you have specified on the Email Notification Server screen (see "Configuring the E-mail Notification Server" on page 6-2).	
	Select one of the following radio buttons to specify the frequency with which the report is sent: <ul style="list-style-type: none"> • Weekly. Reports are sent weekly at the day and time that you specify from the pull-down menus (weekday, hours, and minutes). • Daily. Reports are sent daily at the time that you specify from the pull-down menus (hours and minutes). 	

4. Click **Apply** to save your settings. The Distributed Spam Analysis section and the Send Quarantine Spam Report section each have their own Apply and Reset buttons to enable you to make changes to these sections separately.

Configuring Web and Services Protection

The STM lets you configure the following settings to protect the network's Internet communication:

- The Web protocols that are scanned for malware threats.
- Actions that are taken when infected Web files or objects are detected.
- The maximum file sizes that are scanned.
- Web objects that are blocked.
- Web categories, keywords, and file types that are filtered to block objectionable or high-risk content.
- Domains and URLs that are blocked for objectionable or high-risk content.
- Customer notifications and e-mail alerts that are sent when events are detected.
- Schedules that determine when content filtering is active.

Customizing Web Protocol Scan Settings

If you have used the Setup Wizard, you might have already configured the Web protocol scan settings; the (Web) Policy screen allows you to modify these settings.

Scanning all protocols enhances network security, but might affect the performance of the STM. For an optimum balance between security and performance, only enable scanning of the most commonly used protocols on your network. For example, you can scan FTP and HTTP, but not HTTPS (if this last protocol is not often used). For more information about performance, see [“Performance Management” on page 3-31](#).

To specify the Web protocols and ports that are scanned for malware threats.

1. Select **Web Security > Policies** from the menu. The (Web) Policy screen displays (see [Figure 4-9 on page 4-23](#)).

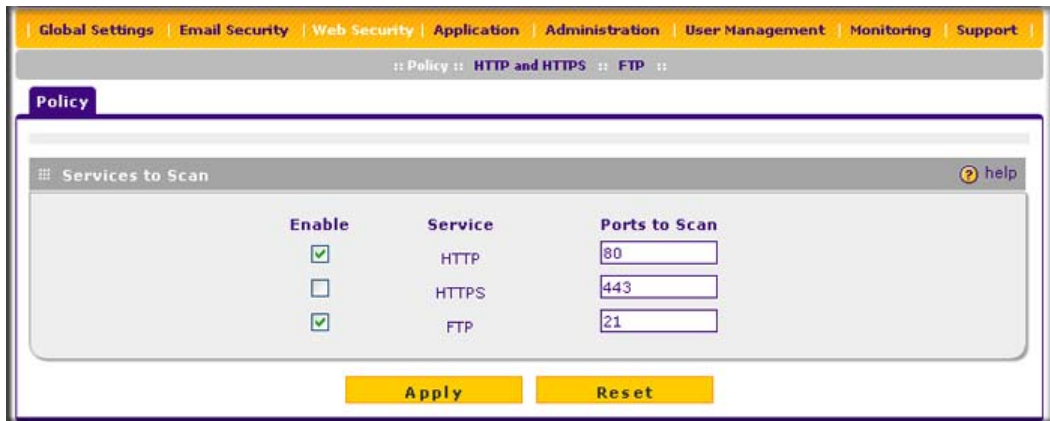



Figure 4-9

- Complete the fields and select the checkboxes as explained in [Table 4-8](#).

Table 4-9. Web Policy Settings

Setting	Description
Services to Scan	
HTTP	Select the HTTP checkbox to enable Hypertext Transfer Protocol (HTTP) scanning. This service is enabled by default and uses default port 80. You can change the standard service port or add another port in the corresponding Ports to Scan field.
HTTPS	Select the HTTPS checkbox to enable Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). This service is disabled by default. The HTTPS default port is 443. You can change the standard service port or add another port in the corresponding Ports to Scan field.
FTP	Select the FTP checkbox to enable File Transfer Protocol (FTP). This service is enabled by default and uses default port 21. You can change the standard service port or add another port in the corresponding Ports to Scan field.

	Note: If a protocol uses a port other than the standard service port (for example, port 80 for HTTP), enter this non-standard port in the Ports to Scan field. For example, if the HTTP service on your network uses both port 80 and port 8080, enter both port numbers in the Ports to Scan field and separate them by a comma.
---	--

- Click **Apply** to save your settings

Configuring Web Malware Scans

If you have used the Setup Wizard, you might have already configured the Web malware action and exception scan settings; the Malware Scan screen allows you to modify these settings.

Whether or not the STM detects Web-based malware threats, you can configure it to take a variety of actions (some of the default actions are listed in [Table 4-1 on page 4-2](#)), skip files that are too large, and send notifications, e-mails, or both to the end users. To configure the Web-based malware settings:

1. Select **Application Security > HTTP/HTTPS** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view.

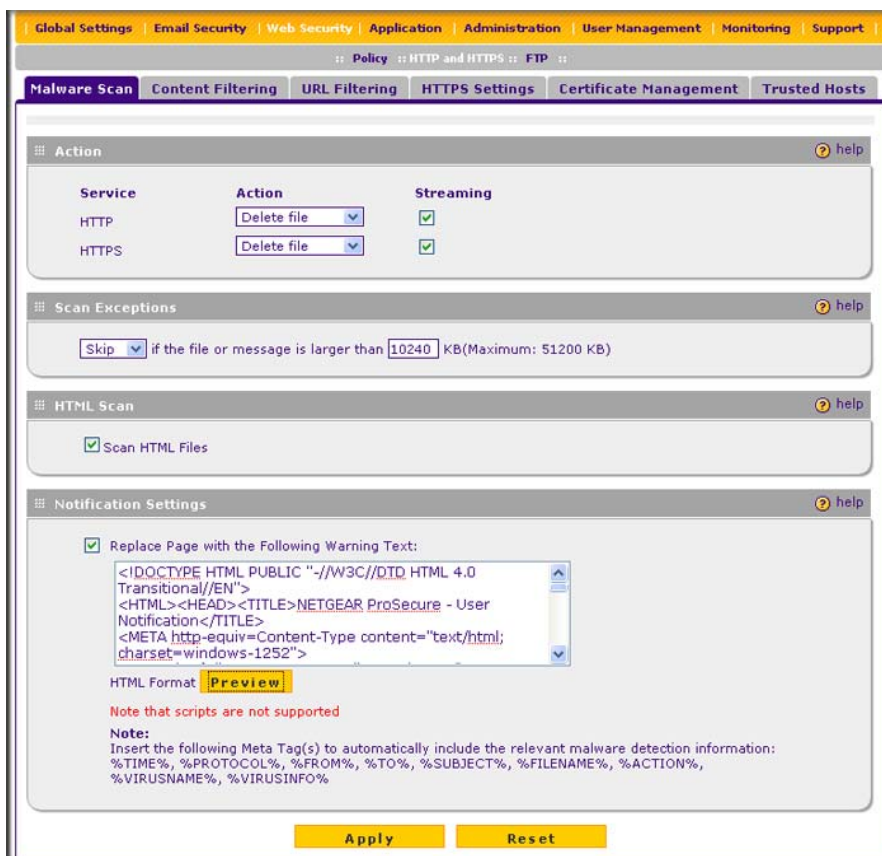


Figure 4-10

2. Complete the fields, select the checkboxes, and make your selections from the pull-down menus as explained in [Table 4-10 on page 4-25](#).

Table 4-10. Malware Scan Settings

Setting	Description	
Action		
HTTP and HTTPS	Action	From the HTTP or HTTPS pull-down menu, specify one of the following actions when an infected Web file or object is detected: <ul style="list-style-type: none"> • Quarantine file. The file is placed in quarantine, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Delete file. This is the default setting. The Web file or object is deleted, and depending on the nature of the malware threat, a virus log entry or a spyware log entry is created. • Log only. depending on the nature of the malware threat, only a virus log entry or a spyware log entry is created. The Web file or object is not placed in quarantine nor deleted.
	Streaming	Select the Streaming checkbox to enable streaming of partially downloaded and scanned HTTP or HTTPS file parts to the end user. This method allows the user to experience more transparent Web downloading. Streaming is enabled by default.
Scan Exceptions		
From the pull-down menu, specify one of the following actions when a file or message exceeds the size that you specify in the file size field: <ul style="list-style-type: none"> • Skip. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • Block. The file is blocked and does not reach the end user. The default and maximum file sizes are: <ul style="list-style-type: none"> • For the STM600 and STM300, the default setting is to block any attachment larger than 10240 KB. The maximum file size that you can specify is 51200 KB. • For the STM150, the default setting is to block any attachment larger than 8192 KB. The maximum file size that you can specify is 25600 KB. Note: Setting the maximum file size to a high value might affect the STM's performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats.		
HTML Scan		
Scan HTML Files	Select this checkbox to enable scanning of HyperText Markup Language (HTML) files, which is enabled by default.	
Notification Settings		
Select the Replace Page with the Following Warning Text checkbox to enable the STM to replace the content of a Web page that is blocked because of a detected malware threat with the following text: NETGEAR ProSecure Web/Email Security Threat Management Appliance has detected and stopped malicious code embedded in this web site for protecting your computer and network from infection. %VIRUSINFO%		

Table 4-10. Malware Scan Settings (continued)

Setting	Description
	<p>Note: You can customize this text. Make sure that you keep the %VIRUSINFO% meta word in the text to enable the STM to insert the proper malware threat information. In addition to the %VIRUSINFO% meta word, you can insert the following meta words in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.</p>
	<p>The text is displayed on the Malware Scan screen with HTML tags. Click Preview to open a screen that displays the notification text in HTML format.</p>

3. Click **Apply** to save your settings.

Configuring Web Content Filtering

If you want to restrict internal LAN users from access to certain types of information and objects on the Internet, use the STM's content filtering and Web objects filtering. With the exception of the Web content categories that are mentioned in [“Default E-mail and Web Scan Settings” on page 4-2](#), all requested traffic from any Web site is allowed. You can specify a message such as “Blocked by NETGEAR” that is displayed on screen if a user attempts to access a blocked site (see the Notification Settings section that is described at the bottom of [Table 4-11 on page 4-30](#)).

Several types of Web content blocking are available:

- **File extension blocking.** You can block files based on their extension. Such files can include, executable files, audio and video files, and compressed files.
- **Web object blocking.** You can block the following Web objects: embedded objects (ActiveX, Java, Flash), proxies, and cookies, and you can disable Java scripts. However, Web sites that are on the whitelist (see [“Configuring Web URL Filtering” on page 4-32](#)) are never subject to Web object blocking.
- **Web category blocking.** You can block entire Web categories because their content is undesired, offensive, or not relevant, or simply to reduce traffic.



Note: You can bypass any type of Web blocking for trusted domains by adding the exact matching domain names to the trusted host list (see [“Specifying Trusted Hosts” on page 4-39](#)). Access to the domains on the trusted host list is allowed for PCs in the groups for which file extension, object, or category blocking, or a combination of these types of Web blocking has been enabled.



Note: You can bypass any type of Web blocking for trusted URLs by adding the URLs to the whitelist (see “[Configuring Web URL Filtering](#)” on page 4-32). Access to the URLs on the whitelist is allowed for PCs in the groups for which file extension, object, or category blocking, or a combination of these types of Web blocking has been enabled.

If you have used the Setup Wizard, you might have already configured the Web category blocking settings; the Content Filtering screen allows you to modify these settings.

To configure Web content filtering:

1. Select **Web Security > HTTP/HTTPS** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view.
2. Click the **Content Filtering** submenu tab. The Content Filtering screen displays. Because of the large size of this screen, it is presented in this manual in three figures ([Figure 4-11](#), [Figure 4-12](#) on page 4-28, and [Figure 4-13](#) on page 4-29).

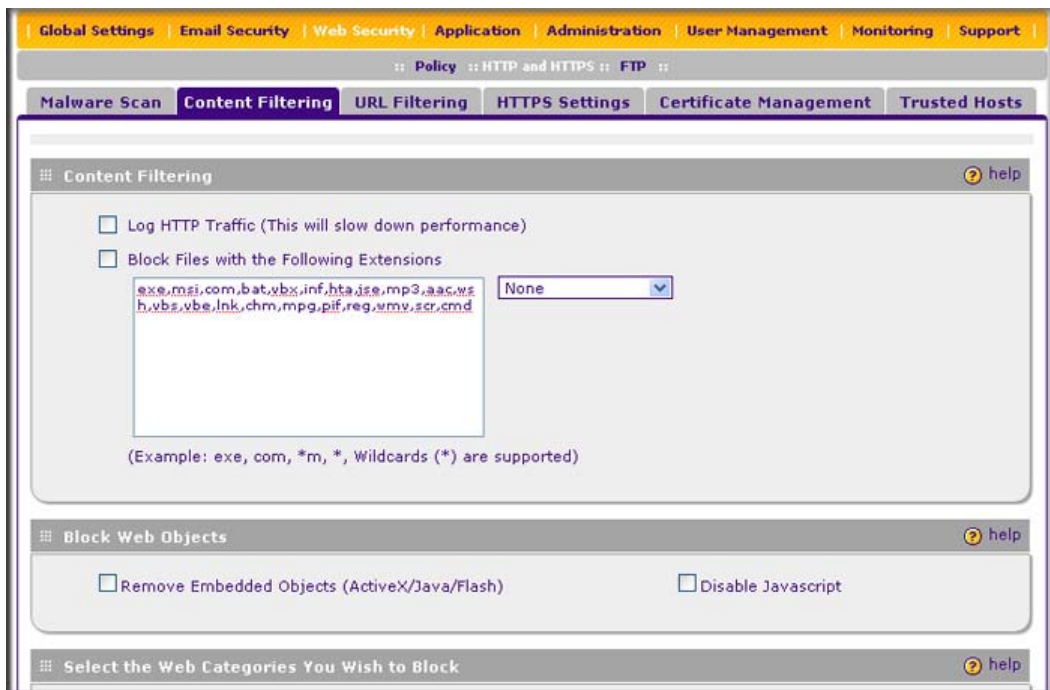


Figure 4-11 [Content Filtering, screen 1 of 3]



Figure 4-12 [Content Filtering, screen 2 of 3]

Web Categorization Schedule help

Do You Want this Schedule to be Active on All Days or Specific Days?

All Days Specific Days

Sunday Monday
 Tuesday Wednesday
 Thursday Friday
 Saturday

Do You Want this Schedule to be Active All Day or at Specific Times during the Day?

All Day Specific Times

Start Time: Hour Minute AM
 End Time: Hour Minute PM

Replace the Content of a Blocked Page with the Following Text help

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html><head><title>NETGEAR ProSecure&#8482 - User Notification</title>
<link href="%STYLE_CSS%" rel="stylesheet" type="text/css">
```

Allow Users to Submit a "Report a URL Misclassification" Form
 (Make sure to include the Meta Tag %SUBMIT-URL-CATEGORIZATION% in the window above)

Insert Link to User Login Portal Page
 (Make sure to include the Meta Tag %LOGIN-LINK% in the window above)

HTML Format **Preview**

Note that scripts are not supported

Note:
 Use "%URL%" to show the URL of the blocked page
 Use "%FULL-CATEGORY-LIST%" to show all the categories that the blocked page falls under

Web Category Lookup help

Enter a URL and press **lookup** to see if it has been categorized

URL:

Lookup Results: Please enter a URL above and click "lookup"

[Click here to Report a URL Misclassification](#)

Figure 4-13 [Content Filtering, screen 3 of 3]

- Complete the fields, select the checkboxes, and make your selections from the pull-down menus as explained in [Table 4-11 on page 4-30](#).

Table 4-11. Content Filtering Settings

Setting	Description
Content Filtering	
Log HTTP Traffic	Select this checkbox to log HTTP traffic. For information about how to view the logged traffic, see “Querying Logs and Generating Reports” on page 6-22 . By default, HTTP traffic is not logged. Note: Logging HTTP traffic might affect the STM's performance (see “Performance Management” on page 3-31).
Block Files with the Following Extensions	Select the checkbox to enable file extension blocking. By default, the File Extension field lists the most common file extensions that are detected. You can manually add or delete extensions. Use commas to separate different extensions. You can also use the pull-down menu to add predefined file extensions from a specific category to the File Extension field: <ul style="list-style-type: none"> • None. No file extensions are added to the File Extension field. This is the default setting. • Executables. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field. • Audio/Video. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field. • Compressed Files. Compressed file extensions (zip, rar, gz, tar, and bz2) added to the File Extension field.
Block Web Objects Select one or both of the following checkboxes:	
Remove Embedded Objects	All embedded objects such as ActiveX, Java, and Flash objects are removed from downloaded Web pages. Note: Because embedded objects are commonly used on legitimate Web sites, blocking embedded objects globally might have a negative impact on a user's Web browsing experience.
Disable Javascript	Javascript is disabled on downloaded Web pages.
Select the Web Categories You Wish to Block	
Select the Enable Blocking checkbox to enable blocking of Web categories, which is the default setting. Select the checkboxes of any Web categories that you want to block. Use the action buttons at the top of the section in the following way: <ul style="list-style-type: none"> • Allow All. All Web categories are allowed. • Block All. All Web categories are blocked. • Set to Defaults. Blocking and allowing of Web categories are returned to their default settings. See Table 4-1 on page 4-2 for information about the Web categories that are blocked by default. Categories that are preceded by a green rectangular are allowed by default; categories that are preceded by a pink rectangular are blocked by default. 	

Table 4-11. Content Filtering Settings (continued)

Setting	Description
Web Categorization Schedule	
Do You Want this Schedule to be Active on All Days or Specific Days?	Select one of the following radio buttons: <ul style="list-style-type: none"> • All Days. The schedule is in effect all days of the week. • Specific Days. The schedule is active only on specific days. To the right of the radio buttons, select the checkbox for each day that you want the schedule to be in effect.
Do You Want this Schedule to be Active All Day or at Specific Times during the Day?	Select one of the following radio buttons: <ul style="list-style-type: none"> • All Day. The schedule is in effect all hours of the selected day or days. • Specific Times. The schedule is active only on specific hours of the selected day or days. To the right of the radio buttons, specify the Start Time and End Time fields (Hour, Minute, AM/PM) during which the schedule is in effect.
Replace the Content of a Blocked Page with the Following Text	
<p>The STM replaces the content of a Web page that is blocked because of violating content with the following text, which you can customize:</p> <p>Internet Policy has restricted access to this location belonging to the following categories: %FULL-CATEGORY-LIST%</p> <p>Note: Make sure that you keep the %FULL-CATEGORY-LIST% meta word in the text to enable the STM to insert all the categories that the blocked Web page falls under. In addition, you can insert the %URL% meta word to show the URL of the blocked page.</p>	
<p>As an option, you can select one or both of the following checkboxes:</p> <ul style="list-style-type: none"> • Allow Users to Submit a "Report a URL Misclassification" Form. When you select this checkbox, the screen that displays when a user attempts to access blocked content includes a hyperlink to report a URL misclassification. See "Click here to Report a URL Misclassification" in the Web Category Lookup section below. <p>Note: Make sure that you keep the %SUBMIT-URL-CATEGORIZATION% meta word in the text to enable the STM to insert the actual hyperlink.</p> • Insert Link to User Login Portal Page. When you select this checkbox, the screen that displays when a user attempts to access blocked content includes a hyperlink that allows the user to log in as another user: <p>You are logged in as %USER% (Click here to login as another user)</p> <p>Note: Make sure that you keep the %LOGIN-LINK% meta word in the text to enable the STM to insert the actual hyperlink.</p> 	
<p>The text is displayed on the Content Filtering screen with HTML tags. Click Preview to open a screen that displays the notification text in HTML format.</p>	


Table 4-11. Content Filtering Settings (continued)

Setting	Description
Web Category Lookup	
URL	Enter a URL to find out if it has been categorized, and if so, in which category. Then, click the lookup button. If the URL has been categorized, the category appears next to Lookup Results.
Clear Web Category Cache	Click Clear Web Category Cache to enable the STM to synchronize with the NETGEAR server and download the most recent Web categorizations. Note: Synchronizing might temporarily slow down the STM's performance because the STM must acquire the Web categorizations remotely instead of from its local cache.
Click here to Report a URL Misclassification	To submit a misclassified or uncategorized URL to NETGEAR for analysis, click on the Click here to Report a URL Misclassification hyperlink. A screen opens that allows you to select from pull-down menus up to two categories in which you think that the URL could be categorized. Then click the Submit button.

4. Click **Apply** to save your settings.

Configuring Web URL Filtering

If you want to allow or block internal LAN users from access to certain sites on the Internet, use the STM's Web URL filtering. You can create or import a whitelist that contains domain names and URLs that are accepted and a blacklist with domain names and URLs that are blocked. The whitelist takes precedence over the blacklist.

	Note: A URL that you enter on the whitelist or blacklist might contain other embedded URLs such as URLs for advertisements or sponsors, causing unexpected behavior. If you want to allow a URL by placing it on the whitelist, make sure that all embedded URLs are also placed on the whitelist. Similarly, if you want to block a URL by placing it on the blacklist, make sure that all embedded URLs are also placed on the blacklist.
---	--

To configure Web URL filtering:

1. Select **Web Security > HTTP/HTTPS** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view.
2. Click the **URL Filtering** submenu tab. The URL Filtering screen displays (see [Figure 4-14 on page 4-33](#)).

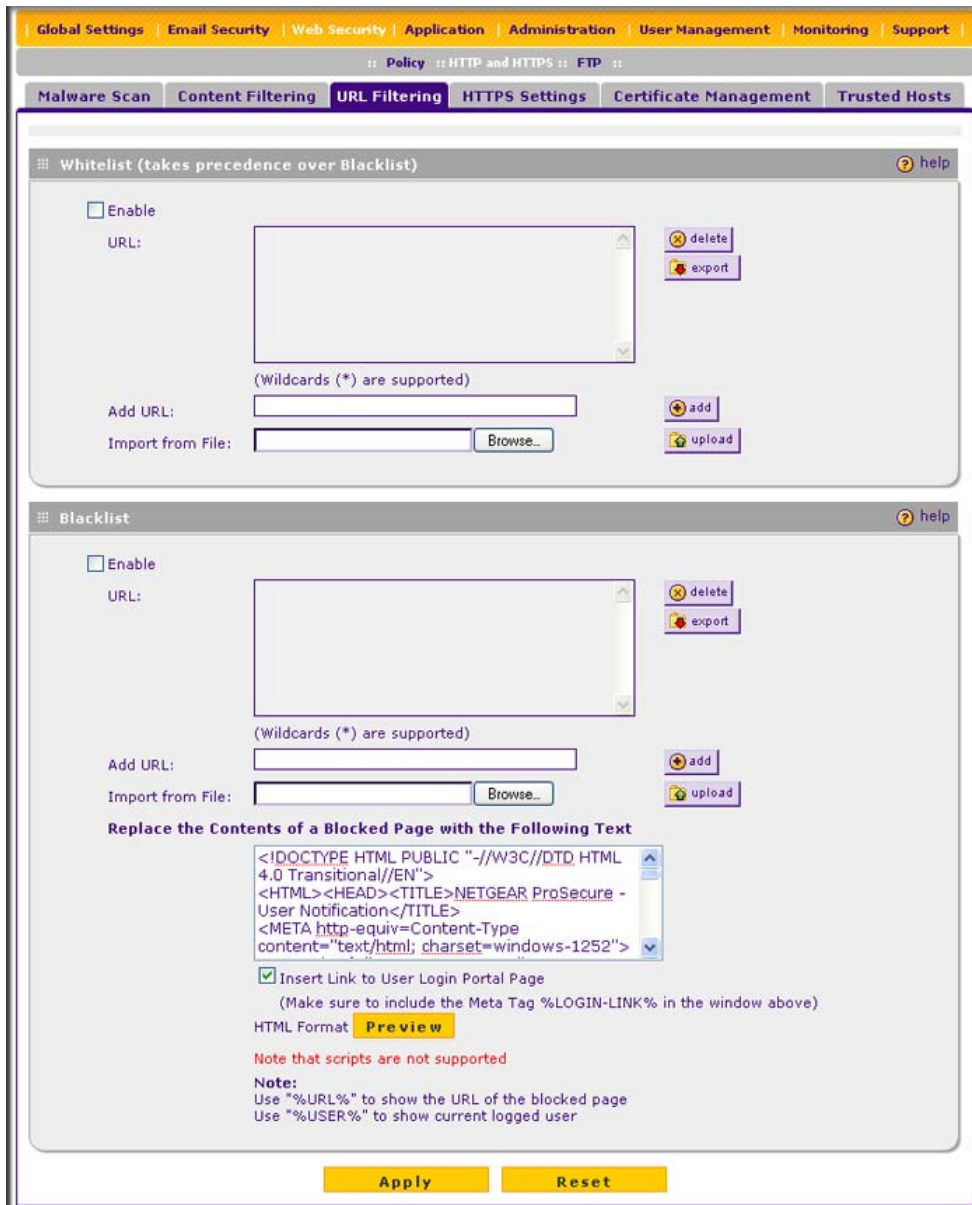


Figure 4-14

3. Complete the fields and select the checkboxes as explained in Table 4-12 on page 4-34.

Table 4-12. URL Filtering Settings

Setting	Description	
Whitelist (takes precedence over Blacklist)		
Enable	Select this checkbox to bypass scanning of the URLs that are listed in the URL field. Users are allowed to access the URLs that are listed in the URL field.	
URL	This field contains the URLs for which scanning is bypassed. To add a URL to this field, use the Add URL field or the Import from File tool (see below). You can add a maximum of 200 URLs. Note: If a URL is in both on the whitelist and blacklist, then the whitelist takes precedence and URLs on the whitelist are not scanned. Note: Wildcards (*) are supported. For example, if you enter “www.net*.com” in the URL field, any URL that begins with “www.net” and ends with “.com” is allowed.	
	delete	To delete one or more URLs, highlight the URLs, and click the delete table button.
	export	To export the URLs, click the export table button and follow the instructions of your browser.
Add URL	Type or copy a URL in the Add URL field. Then, click the add table button to add the URL to the URL field.	
Import from File	To import a list with URLs into the URL field, click the Browse button and navigate to a file in .txt format that contains line-delimited URLs (that is, one URL per line). Then, click the upload table button to add the URLs to the URL field. Note: Any existing URLs in the URL field are overwritten when you import a list of URLs from a file.	
Blacklist		
Enable	Select this checkbox to block the URLs that are listed in the URL field. Users attempting to access these URLs receive a notification (see below).	
URL	This field contains the URLs that are blocked. To add a URL to this field, use the Add URL field or the Import from File tool (see below). You can add a maximum of 200 URLs. Note: If a URL is in both on the whitelist and blacklist, then the whitelist takes precedence and URLs on the whitelist are not scanned. Note: Wildcards (*) are supported. For example, if you enter “www.net*.com” in the URL field, any URL that begins with “www.net” and ends with “.com” is blocked.	
	delete	To delete one or more URLs, highlight the URLs, and click the delete table button.
	export	To export the URLs, click the export table button and follow the instructions of your browser.

Table 4-12. URL Filtering Settings (continued)

Setting	Description
Add URL	Type or copy a URL in the Add URL field. Then, click the add table button to add the URL to the URL field.
Import from File	To import a list with URLs into the URL field, click the Browse button and navigate to a file in .txt format that contains line-delimited URLs (that is, one URL per line). Then, click the upload table button to add the URLs to the URL field. Note: Any existing URLs in the URL field are overwritten when you import a list of URLs from a file.
Replace the Content of a Blocked Page with the Following Text	When a user attempts to access a blocked URL, the STM replaces the content of the blocked URL with the following text, which you can customize: Internet Policy has restricted access to this location: %URL% Note: Make sure that you keep the %URL% meta word in the text to enable the STM to insert the category that the blocked Web page falls under.
	As an option, you can select the Insert Link to User Login Portal Page checkbox to include a hyperlink on screen that allows the user to log in as another user: You are logged in as %USER% (Click here to login as another user) Note: Make sure that you keep the %LOGIN-LINK% meta word in the text to enable the STM to insert the actual hyperlink.
	The text is displayed on the URL Filtering screen with HTML tags. Click Preview to open a screen that displays the notification text in HTML format.

4. Click **Apply** to save your settings.

HTTPS Scan Settings

HTTPS traffic is encrypted traffic that cannot be scanned otherwise the data stream would not be secure. However, the STM can scan HTTPS traffic that is transmitted through an HTTP proxy, that is, HTTPS traffic is scanned as a proxy between the HTTPS client and the HTTPS server.

Figure 4-15 shows the HTTPS scanning traffic flow.

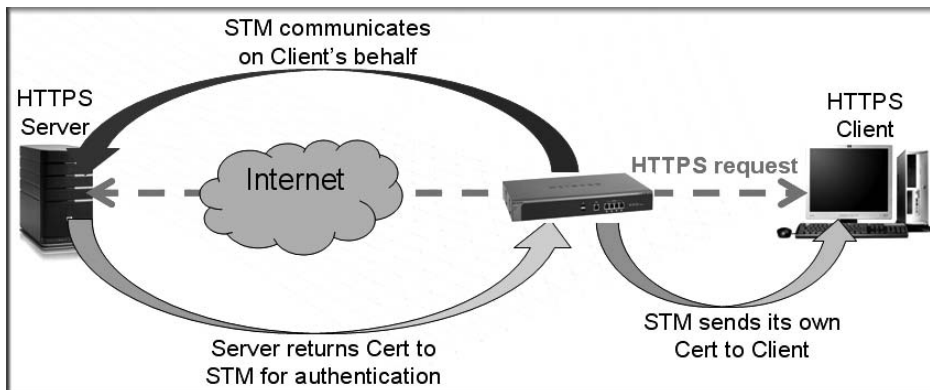


Figure 4-15

The HTTPS scanning process functions with the following principles:

- The STM breaks up an SSL connection between an HTTPS server and an HTTP client in two parts:
 - A connection between the HTTPS client and the STM.
 - A connection between the STM and the HTTPS server.
- The STM simulates the HTTPS server communication to the HTTPS client, including the SSL negotiation, certificate exchange, and certificate authentication. In effect, the STM functions as the HTTPS server for the HTTPS client.
- The STM simulates the HTTPS client communication to the HTTPS server, including the SSL negotiation, certificate exchange, and certificate authentication. In effect, the STM functions as the HTTPS client for the HTTPS server.

During SSL authentication, the HTTPS client authenticates three items:

- Is the certificate trusted?
- Has the certificate expired?
- Does the name on the certificate match that of the Web site?

If one of these is not satisfied, a security alert message appears in the browser window (see [Figure 4-16](#)).



Figure 4-16

However, even when a certificate is trusted or still valid, or when the name of a certificate does match the name of the Web site, a security alert message still appears when a user who is connected to the STM visits an HTTPS site. The appearance of this security alert message is expected behavior because the HTTPS client receives a certificate from the STM instead of directly from the HTTPS server. If you want to prevent this security alert message from appearing, install a root certificate on the client PC. The root certificate can be downloaded from the STM's User Portal Login screen (see [Figure 5-7 on page 5-10](#)).

If client authentication is required, the STM might not be able to scan the HTTPS traffic because of the nature of SSL. SSL has two parts—client and server authentication. HTTPS server authentication occurs with every HTTPS request, but HTTPS client authentication is not mandatory, and rarely occurs. Therefore it is of less importance whether the HTTPS request comes from the STM or from the real HTTPS client.

However, certain HTTPS servers do require HTTPS client certificate authentication for every HTTPS request. Because of the design of SSL, the HTTPS client must present its own certificate in this situation rather than using the one from the STM, preventing the STM from scanning the HTTPS traffic. For information about certificates, see [“Managing Digital Certificates” on page 3-25](#).

You can specify trusted hosts for which the STM bypasses HTTPS traffic scanning. For more information, see [“Specifying Trusted Hosts” on page 4-39](#).

To configure the HTTPS scan settings:

1. Select **Web Security** > **HTTP/HTTPS** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view.
2. Click the **HTTPS Settings** submenu tab. The HTTPS Settings screen displays (see Figure 4-17).

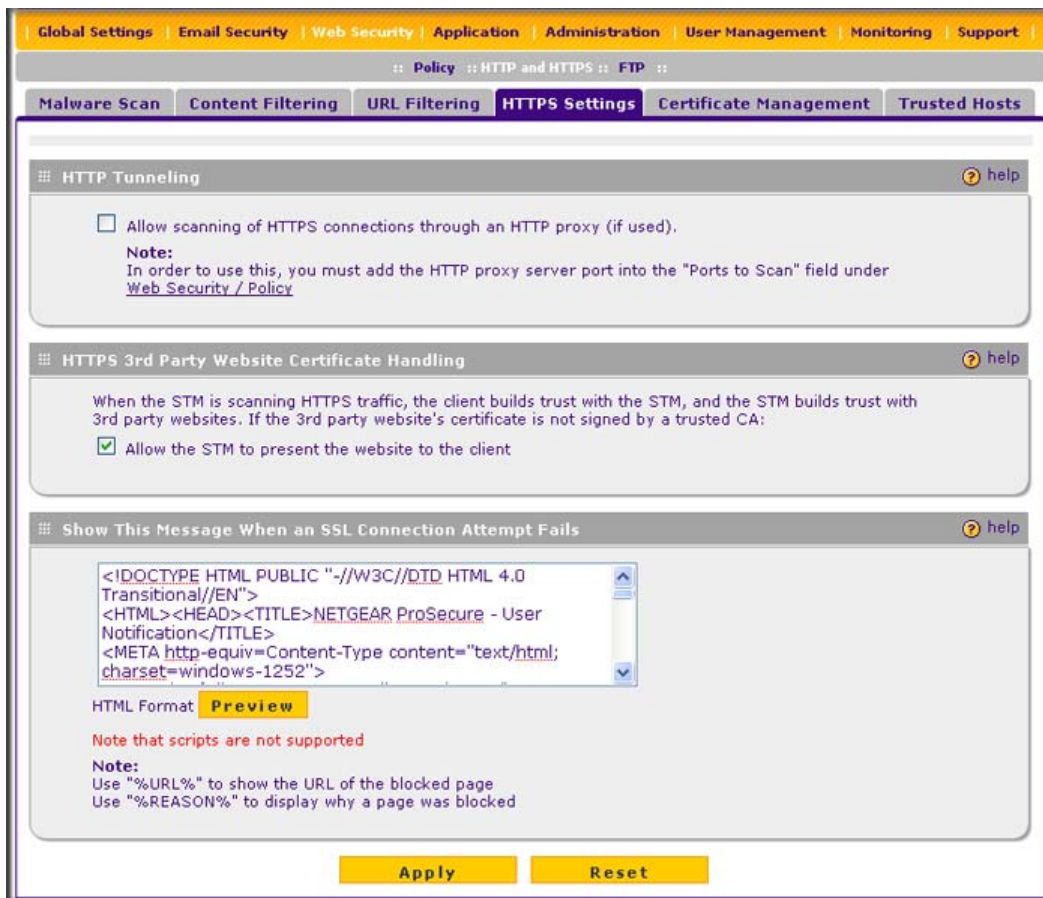



Figure 4-17

3. Complete the fields and select the checkboxes as explained in [Table 4-13](#).

Table 4-13. HTTPS Settings

Setting	Description
HTTP Tunneling	
	Select this checkbox to allow scanning of HTTPS connections through an HTTP proxy, which is disabled by default. Traffic from trusted hosts is not scanned (see “Specifying Trusted Hosts” on page 4-39). Note: For HTTPS scanning to occur properly, you must add the HTTP proxy server port in the Ports to Scan field for the HTTPS service on the Services screen (see “Configuring the HTTP Proxy Settings” on page 3-7).
HTTPS 3rd Party Website Certificate Handling	
	Select this checkbox to allow a Secure Sockets Layer (SSL) connection with a valid certificate that is not signed by a trusted certificate authority (CA). The default setting is to allow such as a connection.
Show This Message When an SSL Connection Attempt Fails	
	By default, a rejected SSL connection is replaced with the following text, which you can customize: The SSL connection cannot be established. URL: %URL% REASON: %REASON% ” Note: The text is displayed on the HTTPS Settings screen with HTML tags. Click Preview to open a screen that displays the notification text in HTML format. Note: Make sure that you keep the %URL% and %REASON% meta words in the text to enable the STM to insert the proper URL information and the reason of the rejection.

4. Click **Apply** to save your settings.

	Note: For information about certificates that are used for SSL connections and HTTPS traffic, see “Managing Digital Certificates” on page 3-25 .
---	---

Specifying Trusted Hosts

You can specify trusted hosts for which the STM bypasses HTTPS traffic scanning and security certificate authentication. The security certificate is sent directly to the client for authentication, which means that the user does not receive a security alert for trusted hosts. For more information about security alerts, see [“Managing Digital Certificates” on page 3-25](#).

Note that certain sites contain elements from different HTTPS hosts. As an example, assume that the `https://example.com` site contains HTTPS elements from the following three hosts:

- `trustedhostserver1.example.com`
- `trustedhostserver2.example.com`
- `imageserver.example.com`

To completely bypass the scanning of the `https://example.com` site, you must add all three hosts to the trusted hosts list because different files from these three hosts are also downloaded when a user attempts to access the `https://example.com` site.

To specify trusted hosts:

1. Select **Web Security** > **HTTP/HTTPS** from the menu. The HTTP/HTTPS submenu tabs appear, with the Malware Scan screen in view.
2. Click the **Trusted Hosts** submenu tab. The Trusted Hosts screen displays.

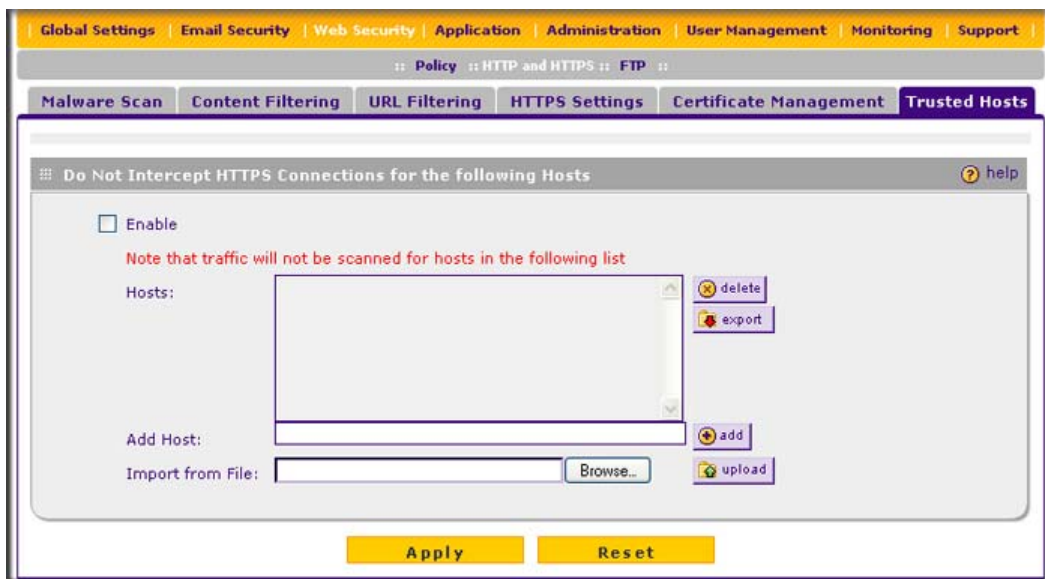


Figure 4-18

- Complete the fields and select the checkbox as explained in [Table 4-14](#).

Table 4-14. Trusted Hosts Settings

Setting	Description
Do Not Intercept HTTPS Connections for the following Hosts	
Enable	Select this checkbox to bypass scanning of trusted hosts that are listed in the Hosts field. Users do not receive a security alert for trusted hosts that are listed in the Host field.
Hosts	This field contains the trusted hosts for which scanning is bypassed. To add a host to this field, use the Add Host field or the Import from File tool (see below). You can add a maximum of 200 URLs.
	delete To delete one or more hosts, highlight the hosts, and click the delete table button.
	export To export the hosts, click the export table button and follow the instructions of your browser.
Add Host	Type or copy a trusted host in the Add Host field. Then, click the add table button to add the host to the Host field.
Import from File	To import a list with trusted hosts into the Host field, click the Browse button and navigate to a file in .txt format that contains line-delimited hosts (that is, one host per line). Then, click the upload table button to add the hosts to the Host field. Note: Any existing hosts in the Host field are overwritten when you import a list of hosts from a file.

- Click **Apply** to save your settings.

Configuring FTP Scans

Some malware threats are specifically developed to spread through the FTP protocol. By default, the STM scans FTP traffic, but you can specify how the STM scans FTP traffic and which action is taken when a malware threat is detected.



Note: The STM does not scan password-protected FTP files.

To configure the FTP scan settings:

- Select **Web Security** > **FTP** from the menu. The FTP screen displays (see [Figure 4-19 on page 4-42](#)).

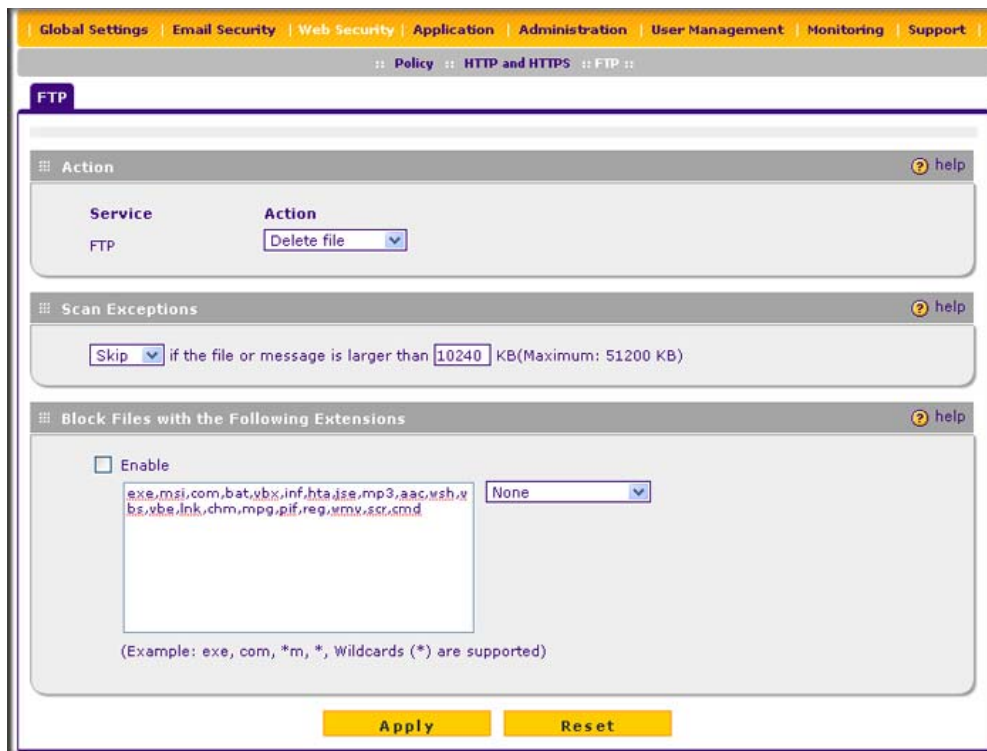


Figure 4-19

2. Complete the fields, select the checkboxes, and make your selections from the pull-down menus as explained in Table 4-15.

Table 4-15. FTP Scan Settings

Setting	Description	
Action		
FTP	Action	<p>From the FTP pull-down menu, specify one of the following actions when an infected FTP file or object is detected:</p> <ul style="list-style-type: none"> • Quarantine file. The FTP file or object is placed in quarantine, a malware quarantine log entry is created, and depending on the nature of the malware threat, also a virus log entry or a spyware log entry. • Delete file. This is the default setting. The FTP file or object is deleted, and depending on the nature of the malware threat, a virus log entry or a spyware log entry is created. • Log only. depending on the nature of the malware threat, only a virus log entry or a spyware log entry is created. The FTP file or object is not deleted.

Table 4-15. FTP Scan Settings (continued)

Setting	Description
Scan Exception	
<p>From the pull-down menu, specify one of the following actions when a file or object exceeds the size that you specify in the file size field:</p> <ul style="list-style-type: none"> • Skip. The file or object is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • Block. The file or object is blocked and does not reach the end user. <p>The default and maximum file sizes are:</p> <ul style="list-style-type: none"> • For the STM600 and STM300, the default setting is to block any file or object larger than 10240 KB. The maximum file size that you can specify is 51200 KB. • For the STM150, the default setting is to block any file or object larger than 8192 KB. The maximum file size that you can specify is 25600 KB. <p>Note: Setting the maximum file size to a high value might affect the STM's performance. NETGEAR recommends the default value, which is sufficient to detect the vast majority of threats.</p>	
Block Files with the Following Extensions	
<p>Select the checkbox to enable file extension blocking. By default, the File Extension field lists the most common file extensions that are detected. You can manually add or delete extensions. Use commas to separate different extensions.</p> <p>You can also use the pull-down menu to add predefined file extensions from a specific category to the File Extension field:</p> <ul style="list-style-type: none"> • None. No file extensions are added to the File Extension field. This is the default setting. • Executables. Executable file extensions (exe, com, dll, so, lib, scr, bat, and cmd) are added to the File Extension field. • Audio/Video. Audio and video file extensions (wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, and aac) are added to the File Extension field. • Compressed Files. Compressed file extensions (zip, rar, gz, tar, and bz2) added to the File Extension field. 	

3. Click **Apply** to save your settings.

Configuring Application Control

The STM lets you control user access to Web applications such as instant messaging, media, peer-to-peer services, and online tools. Blocking an application prohibits all traffic to and from the application, which can be useful when you want to control the STM's throughput. By default, none of the applications are blocked.

To enable and configure application control:

1. Select **Application** from the menu. The Application Control screen displays.

Because of the size of this screen, and because of the way the information is presented, the Application Control screen is divided and presented in this manual in three figures: [Figure 4-20](#) shows only the very top part of the screen, [Figure 4-21 on page 4-45](#) shows the Instant Messaging and Media Application sections, and [Figure 4-22 on page 4-45](#) shows the Peer to Peer and Tools sections.

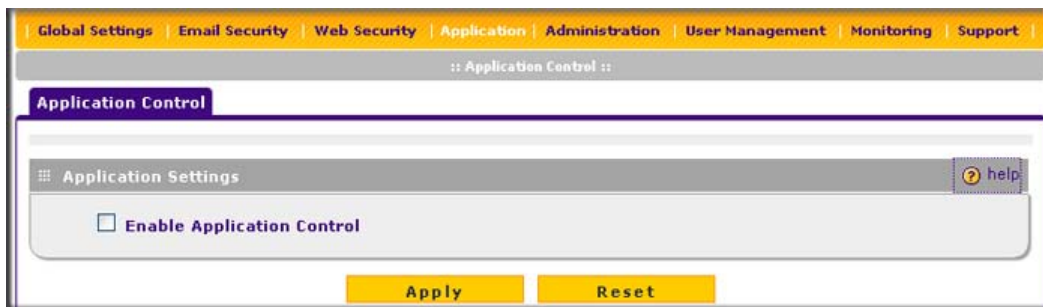


Figure 4-20 [Application Control, screen 1 of 3]

2. In the Application Settings section of the screen, select the Enable Application Control checkbox.
3. Under the Application Settings section of the screen, click **Apply**. The configurations of the individual applications can now take effect.
4. For each of the four application sections on the screen—Instant Messaging, Media Applications, Peer to Peer, and Tools—select the **Block** checkbox to specify to block all applications for that section, or select the individual checkboxes to specify to block individual applications.

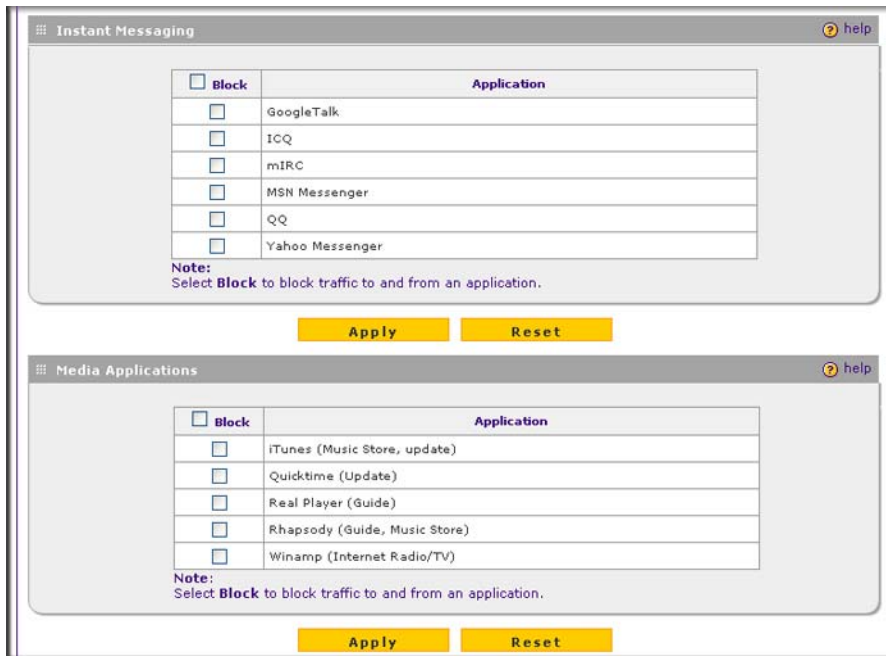


Figure 4-21 [Application Control, screen 2 of 3]

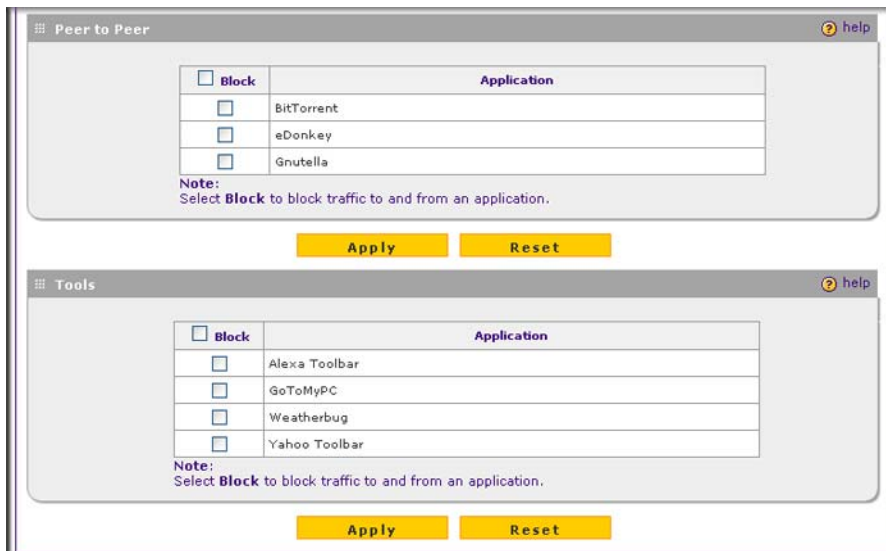


Figure 4-22 [Application Control, screen 3 of 3]

5. After you have configured each section, first click **Apply** to save the settings before you continue with the next section. You must save the configuration changes for each section individually.

For reference, you can specify access control for the following applications:

- Instant Messaging:
 - Google Talk
 - ICQ
 - mIRC
 - MSN Messenger
 - QQ
 - Yahoo Messenger
- Media Applications:
 - iTunes (Music Store, update)
 - Quicktime (Update)
 - Real Player (Guide)
 - Rhapsody (Guide, Music Store)
 - Winamp (Internet Radio/TV)
- Peer to Peer:
 - BitTorrent
 - eDonkey
 - Gnutella
- Tools
 - Alexa Toolbar
 - GoToMyPC
 - Weatherbug
 - Yahoo Toolbar

Setting Scanning Exclusions and Web Access Exceptions

After you have specified which IP addresses and ports the STM scans for malware threats, you can set scanning exclusion rules for certain IP addresses and ports. Similarly, after you have specified which content the STM filters, you can set exception rules for users and members of a group.

Setting Scanning Exclusions

To save resources, you can configure scanning exclusions for IP addresses and ports that you know are secure. For example, if your network includes a Web server that hosts Web pages that are accessible by anyone on the Internet, the files that are hosted by your Web server do not need to be scanned. To prevent the STM from scanning these files, you can configure a scanning exclusion for your Web server.

To configure scanning exclusion rules:

1. Select **Global Settings > Scanning Exclusions** from the menu. The Scanning Exclusions screen displays. This screen shows the Scanning Exclusions table, which is empty if you have not specified any exclusions. (Figure 4-23 shows one exclusion rule in the table as an example.)

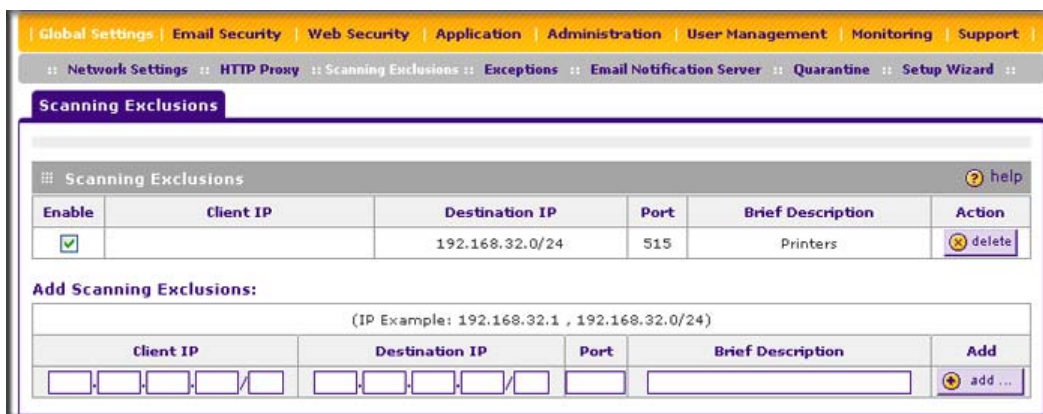


Figure 4-23

2. In the Scanning Exclusions section of the screen, specify an exclusion rule as explained in Table 4-16.

Table 4-16. Add Scanning Exclusion Settings

Setting	Description
Client IP	The client IP address and optional subnet mask that are excluded from all scanning.
Destination IP	The destination IP address and optional subnet mask that are excluded from all scanning.
Port	The port number that is excluded from all scanning.
Brief Description	A description of the exclusion rule for identification and management purposes.

- In the Add column, click the **add** table button to add the exclusion rule to the Scanning Exclusions table. The new exclusion rule is enabled by default.

To disable a rule, select the checkbox in the Enable column for the rule.

To delete an exclusion rule from the Scanning Exclusions table, click the **delete** table button in the Action column to the right of the rule that you want to delete.

Setting Web Access Exception Rules

You can set exception rules for users and members of a group to allow access to applications, Web categories, and URLs that you have blocked for all other users, or the other way around, to block access to applications, Web categories, and URLs that you have allowed access to for all other users. To specify members of a LAN group and to customize LAN group names, see [“Managing Users, Groups, and Authentication” on page 5-1](#).

To set Web access exception rules:

- Select **Global Settings > Exceptions** from the menu. The Exceptions screen displays. This screen shows the Exceptions table, which is empty if you have not specified any exception rules. (Figure 4-24 shows one exception rule in the table as an example.)

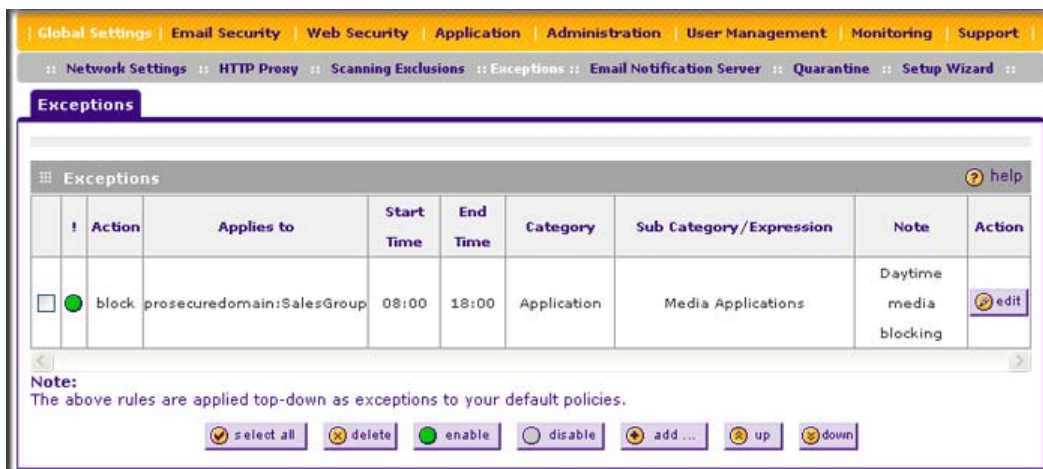


Figure 4-24

- Under the Exceptions table, click the **add** table button to specify an exception rule. The Add Exception screen displays.

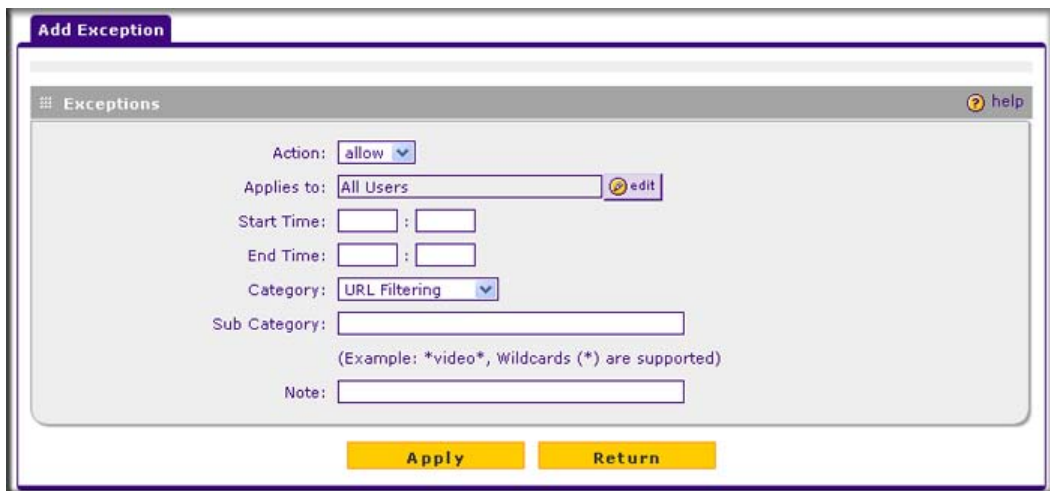


Figure 4-25

- Complete the fields and make your selections from the pull-down menus as explained in Table 4-17.

Table 4-17. Add Exception Settings

Setting	Description
Action	From the pull-down menu, select the action that the STM applies: <ul style="list-style-type: none"> allow. The exception allows access to an application, Web category, or URL that is otherwise blocked. block. The exception blocks access to an application, Web category, or URL that is otherwise allowed.
Applies to	Click the edit button to open the “Applies to” screen that lets you configure a domain, group, or individual user to which the exception must apply (see the screen below, in the table). If applicable, on the “Applies to” screen, click a lookup button to retrieve a domain, group, or user. When you have made your decision, click an Apply button to add the domain, group, or user to the Applies to field on the Add Exception screen. The options on the “Applies to” screen are explained below.

Table 4-17. Add Exception Settings (continued)

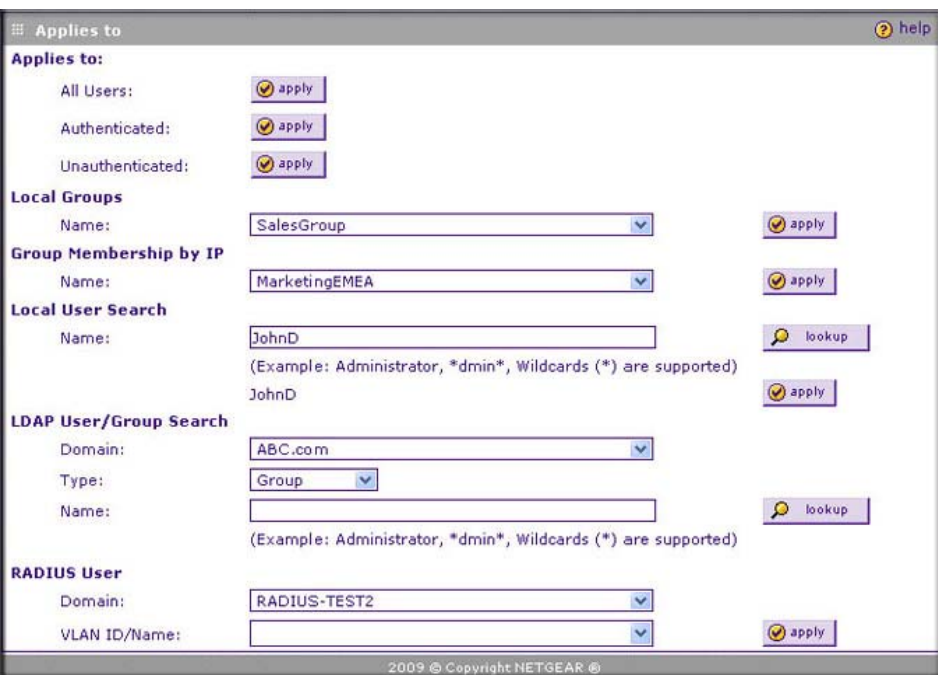
Setting	Description
Applies to (continued)	
All Users	Click the apply button to apply the exception to all users, both authenticated and unauthenticated.
Authenticated	Click the apply button to apply the exception to all authenticated users. These are users who have actively logged in to the STM and who have been authenticated.
Unauthenticated	Click the apply button to apply the exception to all unauthenticated users. These are users who have not actively logged in to the STM. By default, these users are assigned the account name "anonymous".
Local Groups	<p>Do the following:</p> <ol style="list-style-type: none"> 1. From the Name pull-down menu, select a local group. 2. Click the apply button to apply the exception to the selected local group. <p>You can specify local groups on the Groups screen (see “Creating and Deleting Groups by Name” on page 5-3).</p>

Table 4-17. Add Exception Settings (continued)

Setting	Description
Applies to (continued)	Group Membership by IP Do the following: 1. From the Name pull-down menu, select a group that is defined by its IP address. 2. Click the apply button to apply the exception to the selected group. You can specify groups that are defined by their IP address on the IP/Subnet Groups screen (see “Creating and Deleting Groups by IP Address and Subnet” on page 5-5).
	Local User Search Do the following: 1. In the Name field, enter a user name. 2. Click the lookup button. If the user is found, they are listed to the left of the apply button. 3. Click the apply button to apply the exception to the selected user.
	LDAP User/Group Do the following: 1. From the Domain pull-down menu, select an LDAP domain. 2. From the Type pull-down menu, select User , Group , or User&Group . 3. In the Name field, enter the name of the user, group, or user and group. 4. Click the lookup button. If the user or group is found, they are listed to the left of the apply button. 5. Click the apply button to apply the exception to the selected user or group. You can specify LDAP domains, groups, and users on the LDAP screen (see “Creating and Deleting LDAP and Active Directory Domains” on page 5-16).
	RADIUS User Do the following to specify a RADIUS domain to which the exception applies: 1. From the Domain pull-down menu, select a RADIUS domain. 2. From the VLAN ID/Name pull-down menu, select a VLAN ID or VLAN name. 3. Click the apply button to apply the exception to the selected VLAN. You can specify RADIUS domains and VLANs on the RADIUS screen (see “Creating and Deleting RADIUS Domains” on page 5-19).
Start Time	The time in 24-hour format (hours and minutes) when the action starts. If you leave these fields empty, the action applies continuously.
End Time	The time in 24-hour format (hours and minutes) when the action ends. If you leave these fields empty, the action applies continuously.

Table 4-17. Add Exception Settings (continued)

Setting	Description
Category	From the pull-down menu, select the category to which the action applies: <ul style="list-style-type: none"> • URL Filtering. The action applies to a URL. Enter the URL in the Subcategory field. • Web category. The action applies to a Web category. Select a category from the Subcategory pull-down menu. • Application. The action applies to an application. Select an application from the Subcategory pull-down menu.
Subcategory	The nature of the Subcategory field depends on your selection from the Category pull-down menu. <ul style="list-style-type: none"> • When you select URL Filtering: The Subcategory field becomes a blank field in which you can enter a full or partial URL. • When you select Web category: The Subcategory field becomes a pull-down menu that lets you select a Web category. • When you select Application: The Subcategory field becomes a pull-down menu that lets you select an application.
Notes	A description of the exception rule for identification and management purposes or any other relevant information that you wish to include.

4. Click **Apply** to save your settings. The new exception rule is added to the Exceptions table. To return to the Exception screen without adding the rule, click **Return**.
5. Select the checkbox to the left of the rule that you want to enable or click the **select all** table button to select all rules.
6. Click the **enable** table button to enable the selected rule or rules.

To make changes to an existing exception rule:

1. In the Action column to the right of to the exception rule, click the **edit** table button. The Edit Exception screen displays. This screen is identical to the Add Exception screen (see [Figure 4-24 on page 4-48](#)).
2. Modify the settings that you wish to change (see [Table 4-17 on page 4-49](#)).
3. Click **Apply** to save your changes. The modified exception rule is displayed in the Exceptions table.

To delete or disable one or more exception rules:

1. Select the checkbox to the left of the rule that you want to delete or disable or click the **select all** table button to select all rules.

2. Click one of the following table buttons:

- **disable.** Disables the rule or rules. The “!” status icon changes from a green circle to a grey circle, indicating that the rule is or rules are disabled. (By default, when a rule is added to the table, it is automatically enabled.)
- **delete.** Deletes the rule or rules.

The table rank of the exception rule in the Exceptions table determines the order in which the rule is applied (from the top down). To change the position of the rules in the table, select one or more rules, and then click one of the following table buttons:

- **up.** Moves the rule or rules up one position in the table rank.
- **down.** Moves the rule or rules down one position in the table rank.

Chapter 5

Managing Users, Groups, and Authentication

This chapter describes how to manage users, groups, and authentication on the STM. This chapter contains the following sections:

- [“About Users, Groups, and Domains”](#) on this page.
- [“Configuring Groups”](#) on page 5-2.
- [“Configuring User Accounts”](#) on page 5-6.
- [“Configuring Authentication”](#) on page 5-9.
- [“Global User Settings”](#) on page 5-24.
- [“Viewing and Logging Out Active Users”](#) on page 5-25.

About Users, Groups, and Domains

Users can be individual users or can be part of a group, and a group is generally part of a domain. Normally, you first create a domain, then you create a group that you assign to a domain, and then you create users that you assign to a group. The STM does not let you create domains; the local groups that you define are automatically assigned to the STM’s `prosecuredomain` default domain. However, you can use existing LDAP and RADIUS domains on the STM.

The main purpose for using groups and domains is to apply exceptions (that is, adding or removing restrictions) for Web browsing, URL access, and application access (see [“Setting Web Access Exception Rules”](#) on page 4-48).



Note: For information about a different type of users—those with administrative and guest privileges—see [“About Users with Administrative and Guest Privileges”](#) on page 3-9.

The STM supports both unauthenticated and authenticated users:

- **Unauthenticated users.** Anonymous users who do not log in to the STM and to which the STM’s default e-mail and Web access policies apply.

- **Authenticated users.** User who have a computer behind the STM, who log in to the STM with a user name and password, and who are assigned an access policies that normally differs from the STM's default e-mail and Web access policies. Different users or user groups can have different access policies, so there can be multiple access policies on the STM.

In addition to being authenticated as individual users, users can be authenticated on the STM according to group membership or IP address:

- Group membership. A group is defined in the STM's local database, an LDAP database, or a RADIUS database. If you use a RADIUS database for authentication, a group can also be defined in a VLAN.
- IP address. A group is defined by its IP address and subnet.



Note: For detailed information about authentication, see [“Configuring Authentication” on page 5-9](#).

The login window that is presented to this type of users is the User Portal Login screen (see [Figure 5-7 on page 5-10](#)), which requires three items: a user name, a password, and a domain selection. The domain determines the authentication method that must be used—LDAP, Active Directory, RADIUS, or the STM's local database.

Configuring Groups

The use of groups simplifies the application of exception policies that allow different sets of users to have different Internet access restrictions. Rather than applying the same exception to each user, it is easier to apply a single exception to the entire group. For information about exception policies, see [“Setting Web Access Exception Rules” on page 4-48](#).

You can define groups either by name or by IP address and subnet:

- **Groups defined by name.** These are local groups on the STM to which you can add users from the STM's local user database. Local groups are automatically assigned to the STM's prosecuredomain default domain.



Note: For information about groups that are defined by VLANs, see [“Creating and Deleting VLANs for Use with RADIUS Domains” on page 5-23](#).

- **Groups defined by IP address and subnet.** These are groups that can be on your local network or on a remote device.



Note: If you use groups on a remote device, you must configure your network's firewall to allow access to the IP address and subnet mask that have been assigned to the remote group.

Creating and Deleting Groups by Name

To create a local group by name:

1. Select **User Management > Groups** from the menu. The Groups screen displays (Figure 5-1 contains one example).

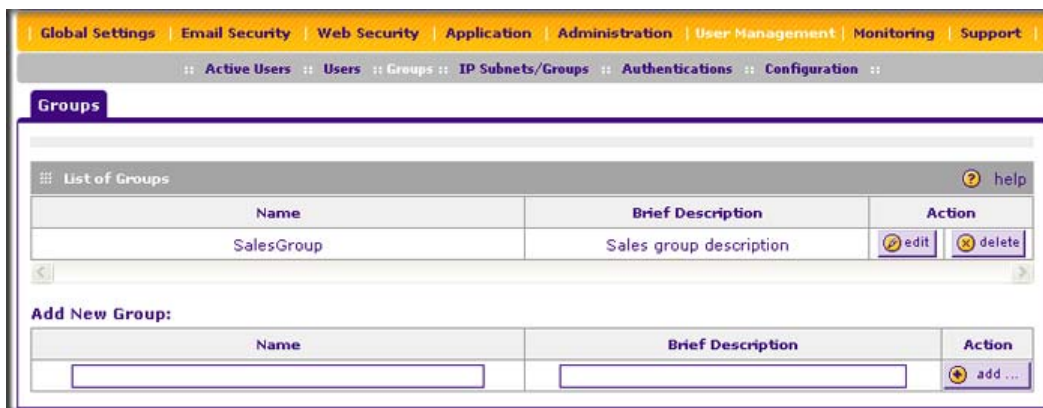


Figure 5-1

The List of Groups table displays the local groups with the following fields:

- **Name.** The name of the group, which is the defining characteristic of the group.
 - **Brief Description.** An optional brief description of the group.
 - **Action.** The edit table button that provides access to the Edit Group screen and the delete table button that allows you to delete the group.
2. In the Add New Group section of the screen, complete the fields as explained in Table 5-1.

Table 5-1. Group Settings

Setting	Description
Name	A descriptive (alphanumeric) name of the group for identification and management purposes.
Description	A brief description of the group for identification and management purposes. This description is optional.

3. Click the **add** table button. The new group is added to the List of Groups table.

To delete a group from the List of Groups table, click the **delete** table button in the Action column for the group that you want to delete.



Note: When you delete a group, an exception rule that is associated with this group no longer has any effect. You can delete such an exception rule.

Editing Groups by Name

To edit a local group that you created by name:

1. Select **User Management > Groups** from the menu. The Groups screen displays (see [Figure 5-1 on page 5-3](#)).
2. In the Action column of the List of Groups table, click the **edit** table button for the group that you want to edit. The Group Edit screen displays ([Figure 5-2](#) contains some examples).

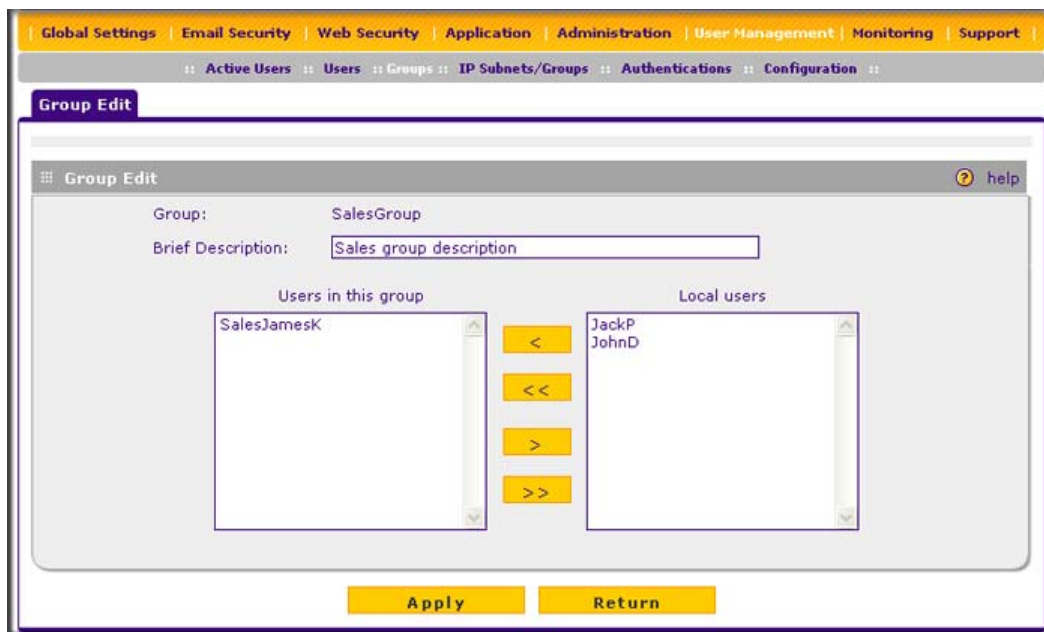


Figure 5-2

3. Change the field and move the users as explained in [Table 5-2 on page 5-5](#).

Table 5-2. Group Edit Settings

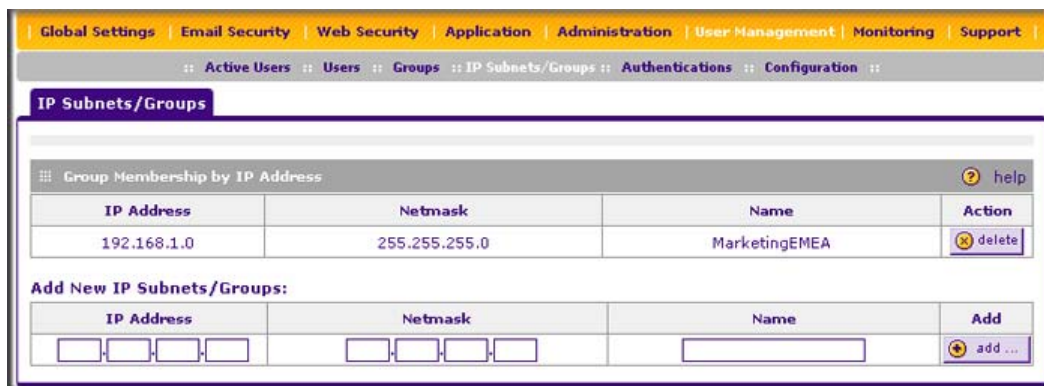
Setting	Description
Edit Description	You can edit the brief description of the group for identification and management purposes.
	To move users from one field to another, use one of the following methods: <ul style="list-style-type: none"> • Move a single user: highlight the users, then click a single arrow button to move the user from one field to the other. • Move all users: click a double arrow button to move all users from one field to the other.
Users in this group	The users that you previously added to this group.
Local users	All local users that are not part of the group.

4. Click **Apply** to save your changes.

Creating and Deleting Groups by IP Address and Subnet

To create a group by IP address and subnet:

1. Select **User Management > IP Subnet/Groups** from the menu. The IP Subnet/Groups screen displays (Figure 5-3 contains one example).

**Figure 5-3**

The Groups Membership by IP Address table displays the groups with the following fields:

- **IP Address.** The IP address for the group.
- **Netmask.** The subnet mask for the group.
- **Name.** The name of the group.
- **Action.** The delete table button that allows you to delete the group.

2. In the Add New IP Subnets/Groups section of the screen, complete the fields as explained in [Table 5-3](#).

Table 5-3. IP Subnet/Group Settings

Setting	Description
IP Address	An IP address on your local network or on a remote device to which the users are assigned.
Netmask	The subnet mask to which the users are assigned. For an individual IP address, specify 255.255.255.255.
Name	A descriptive (alphanumeric) name of the group for identification and management purposes.

3. Click the **add** table button. The new group is added to the Groups Membership by IP Address table.

To delete a group from the List of Groups table, click the **delete** table button in the Action column for the group that you want to delete.



Note: When you delete a group, an exception rule that might be associated with this group no longer has any effect. You can delete such an exception rule.

Configuring User Accounts

When you create a user account, you can assign the user to a local group. Therefore, you should first create any local groups, then user accounts. User accounts are added to the STM's local user database.

Creating and Deleting User Accounts

To create an individual user account:

1. Select **Users > Users** from the menu. The Users screen displays ([Figure 5-4 on page 5-7](#) contains some examples).

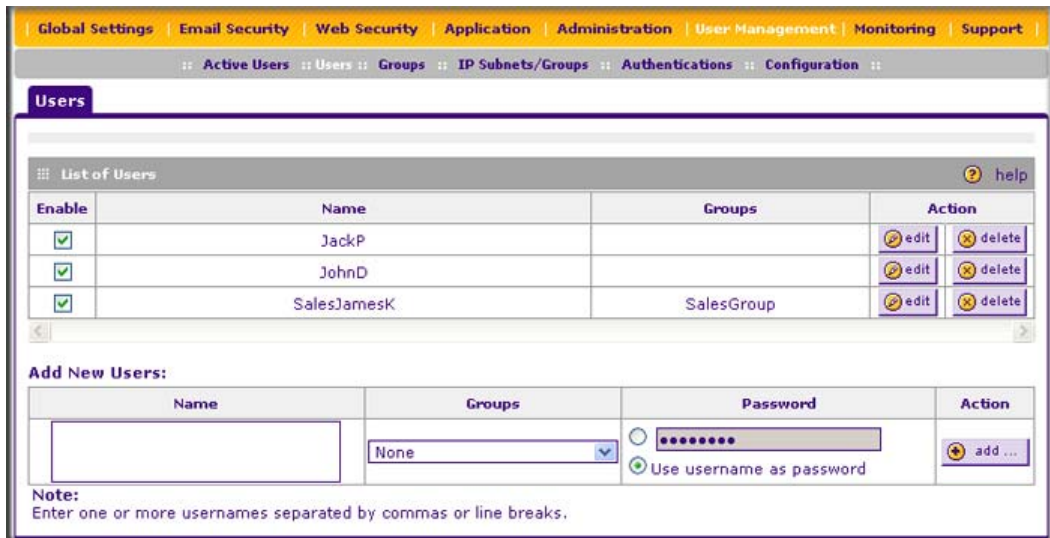


Figure 5-4

The List of Users table displays the users with the following fields:

- **Enable.** The checkbox allows you to enable or disable the user.
 - **Name.** The name of the user.
 - **Group.** The group to which the user is assigned. If no group is displayed, the user is not assigned to any group.
 - **Action.** The edit table button that provides access to the Edit User screen and the delete table button that allows you to delete the user.
2. In the Add New Users section of the screen, complete the fields, make your selection from the pull-down menu, and select the radio buttons as explained in [Table 5-4](#).

Table 5-4. User Settings

Setting	Description
Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
Groups	The pull-down menu shows the local groups that are listed on the Group screen. From the pull-down menu, select the group to which the user is assigned. For information about how to configure groups, see “Configuring Groups” on page 5-2 .

Table 5-4. User Settings (continued)

Setting	Description
Password	Select one of the following radio buttons: <ul style="list-style-type: none"> • The radio button to the left of the Password field. Enter the password that the user must enter to gain access to the STM. The password can be up to 64 characters. • Use username as the password. The password that is assigned to the user is identical to the user name.

3. Click the **add** table button. The new user is added to the List of Users table.

To delete a user from the List of Users table, click the **delete** table button in the Action column for the user that you want to delete.

Editing User Accounts

The only field that you can change for a user account is the password. To modify the password for a user:

1. Select **Users > Users** from the menu. The Users screen displays (see [Figure 5-4 on page 5-7](#)).
2. Click the **edit** table button in the Action column for the user whose password you want to modify. The Edit User screen displays ([Figure 5-5](#) contains an example).

Figure 5-5

3. Modify the password:
 - a. In the Password field, enter the new password.
 - b. In the Confirm Password field, repeat the new password.
4. Click **Apply** to save your settings.

Configuring Authentication

The login screen and authentication on the STM depends on the user type and the authentication method:

- **Administrative users.** Users with administrative and guest privileges on the STM must log in through the NETGEAR Configuration Manager Login screen (see [Figure 5-6](#)) where they are authenticated through the STM's local user database. These users must provide their user name and password.

For information about the pre-defined administrator and guest user accounts, see “[About Users with Administrative and Guest Privileges](#)” on page 3-9. To change the administrator default name and password or guest default name and password, see “[Changing Administrative Passwords and Timeouts](#)” on page 3-9.

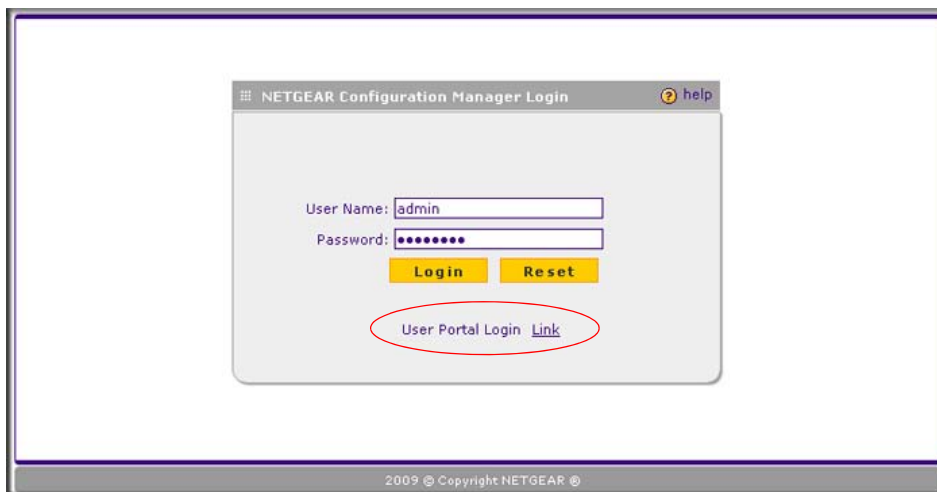
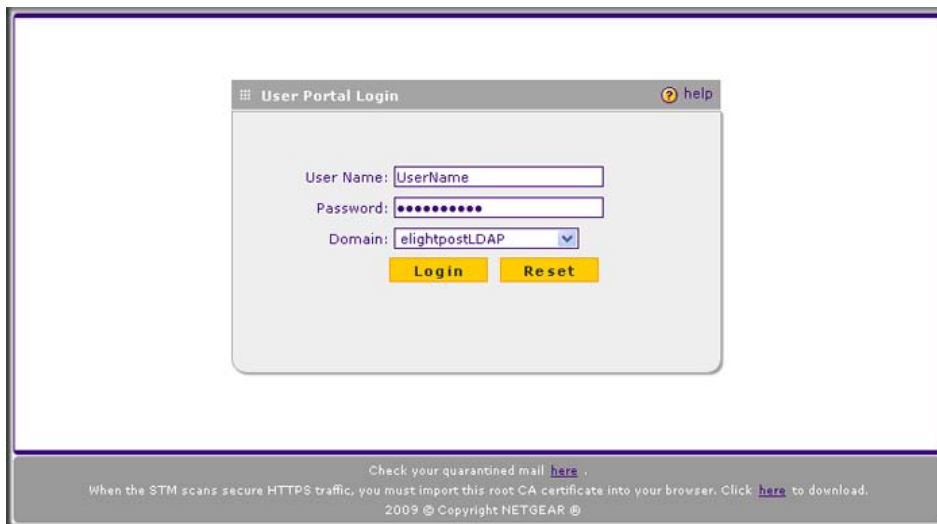


Figure 5-6

- **Users with special access privileges.** User who have a computer behind the STM and who are assigned access policies that differ from the STM's default e-mail and Web access policies (see “[Setting Web Access Exception Rules](#)” on page 4-48) must log in through the User Portal Login screen (see [Figure 5-7](#) on page 5-10). These users must provide their user name, password, and select the domain to which they have been assigned.

The lower part of the NETGEAR Configuration Manager Login screen (see [Figure 5-6](#)) provides a User Portal Login Link.



The screenshot shows the 'User Portal Login' interface. It features a header with a menu icon and a 'help' link. The main form contains three input fields: 'User Name' with the value 'UserName', 'Password' with masked characters, and 'Domain' with a dropdown menu set to 'elightpostLDAP'. Below the fields are two yellow buttons: 'Login' and 'Reset'. At the bottom of the page, there is a footer with text: 'Check your quarantined mail. [here](#). When the STM scans secure HTTPS traffic, you must import this root CA certificate into your browser. Click [here](#) to download. 2009 © Copyright NETGEAR ©'.

Figure 5-7

After a user has logged in through the User Portal Login screen, the Authentication screen displays.




The screenshot shows the 'Authentication' screen. At the top, a red message states: 'You have successfully logged in from IP : 192.105.155.84'. Below this is a header with an 'Edit' menu icon and a '[Logout]' button circled in red, along with a 'help' link. The main form contains three input fields: 'Name' with the value 'JohnD', 'Password' with masked characters, and 'Confirm Password' which is empty. Below the fields is a yellow 'Apply' button. At the bottom of the page, there is a footer with text: '2009 © Copyright NETGEAR ©'.

Figure 5-8


The Authentication screen shows the IP address with which the user has logged in and lets a user change the password.

After completing a session, a user must log out by following these steps:

- a. Return to the User Portal Login screen (see [Figure 5-7](#)).

	<p>The user must know how to return to the User Portal Login screen. The administrator must provide the User Portal Login URL: https://<IP_address>/~common/cgi-bin/user_login.pl or https://<FullyQualifiedDomainName>/~common/cgi-bin/user_login.pl</p> <p>Alternately, the administrator can provide the NETGEAR Configuration Manager Login screen, from where the user can access the User Portal Login screen: https://<IP_address> or https://<FullyQualifiedDomainName></p>
---	---

- b. Log in again.
- c. On the Authentication screen (see [Figure 5-8 on page 5-10](#)), click the **logout** link.

	<p>Warning: Ensure that users understand that they must log out after completing a session in order to prevent subsequent users from inheriting access privileges that were not assigned to them.</p>
---	--

In addition to authentication through the STM's local user database, the STM supports the following external authentication methods for users logging in through the User Portal Login screen:

- **LDAP.** A network-validated domain-based authentication method that functions with a Lightweight Directory Access Protocol (LDAP) authentication server. LDAP is a standard for querying and updating a directory. Because LDAP supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on LDAP attributes.
- **Active Directory.** A network-validated domain-based authentication method that functions with a Microsoft Active Directory authentication server. Microsoft Active Directory authentication servers support a group and user structure. Because the Active Directory supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on Active Directory attributes. A Microsoft Active Directory database uses an LDAP organization schema.
- **RADIUS.** A network-validated PAP or CHAP password-based authentication method that functions with Remote Authentication Dial In User Service (RADIUS).

RADIUS support two types of protocols:

- **PAP.** Password Authentication Protocol (PAP) is a simple protocol in which the client sends a password in clear text.
- **CHAP.** Challenge Handshake Authentication Protocol (CHAP) executes a three-way handshake in which the client and server trade challenge messages, each responding with a hash of the other’s challenge message that is calculated using a shared secret value.

When logging in through the User Portal Login screen, users must provide their name and password, and select the domain that corresponds to the authentication method that has been assigned to them.

Understanding Active Directories and LDAP Configurations

This manual assumes that you already have a knowledge of Active Directories and LDAP servers. The following sections are meant to provide some additional information before you go to [“Creating and Deleting LDAP and Active Directory Domains”](#) on page 5-16.

How an Active Directory Works

Understanding how a typical Active Directory (AD) works might be of help when specifying the settings for the LDAP and Active Directory domains on the STM.

The following applies to a typical AD:

- Organizational unit (ou), common name (cn), and domain controller (dc) can all be used to build a search base in the AD. The following applies to the ‘ou’ and ‘cn’ containers:
 - An AD administrator can create an ou but cannot create a cn that was built in the AD server.
 - An AD administrator can apply a global policy objects (gpo) to an ou, but not to a cn.
- An ou is created in the root node (for example, dc=companyname, dc=com) of the hierarchy. In a company AD, an ou often represents a regional office or department.
- A groups is created under cn=users.
- A users is created under each ou so that the user can logically show in a tree of the AD server.
- A relationship between a group and users is built using their attributes (by default: member and memberOf). These show in a lookup result.

The following is an example of how to set the search base:

If in a company AD server “cn=users” and “ou=companyname” and both are specified under “dc=companyname,dc=com”, the search base must be set as “dc=companyname,dc=com” in order to search both users and groups.

If the size limit is exceeded so that “dc=companyname,dc=com” misses some entries during the lookup process, a user can still be properly authenticated. However, to prevent the size limit from being exceeded, an AD administrator must set a larger value in the LDAP server configuration so that the entire list of users and groups is returned in the lookup result. Another workaround is to use a specific search name or a name with a wildcard in the lookup process, so that the subset of the entire list is returned in the lookup result.

How to Bind a ‘dn’ in an LDAP Configuration

Understanding how to bind a distinguished name (dn) in an LDAP configuration might be of help when specifying the settings for the LDAP and Active Directory domains on the STM.

In this example, the LDAP domain name is “ABC.com” and the LDAP server has IP address 192.168.35.115 on port 389. To bind a user with the name Jamie Hanson with the LDAP server:

1. On a computer that has access to the Active Directory (AD), open the Active Directory for Users and Computers.
2. Select the user Jamie Hanson.
3. Click the General tab. The general properties for Jamie Hanson display.

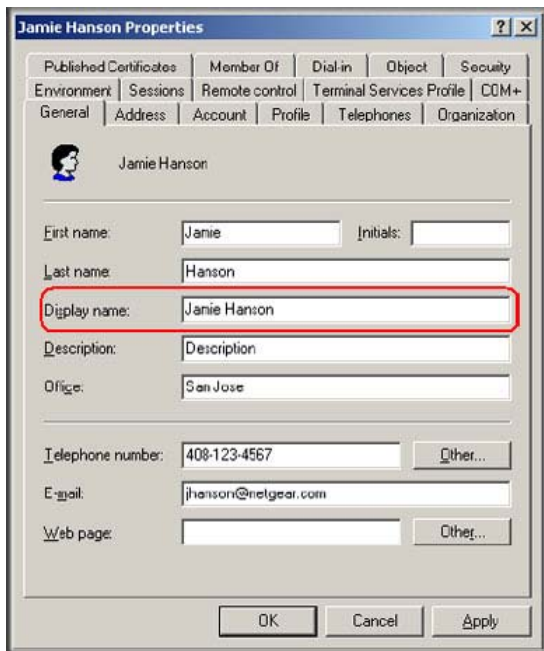


Figure 5-9

- To verify Jamie Hanson's user logon name, click the Account tab. The account properties for Jamie Hanson display.

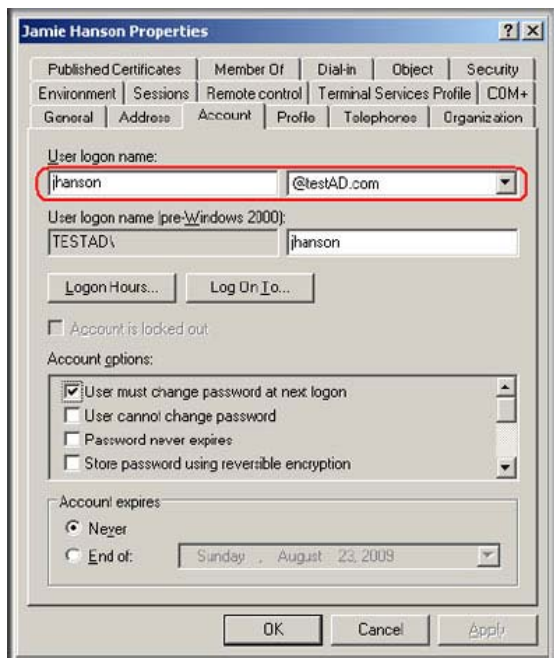


Figure 5-10

- Log in to the STM.
- Select **User Management > Authentications** from the menu The LDAP screen displays.
- In the List of LDAP table, click the **edit** button on in the Action column of domain ABC.com. The Edit LDAP screen displays.
- To bind the user Jamie Hanson to the LDAP server for authentication on the STM, use any one of the following three formats in the Bind DN field of the Edit LDAP screen:
 - The display name in dn format:
cn=Jamie Hanson,cn=users,dc=testAD,dc=com (see [Figure 5-11 on page 5-15](#)).

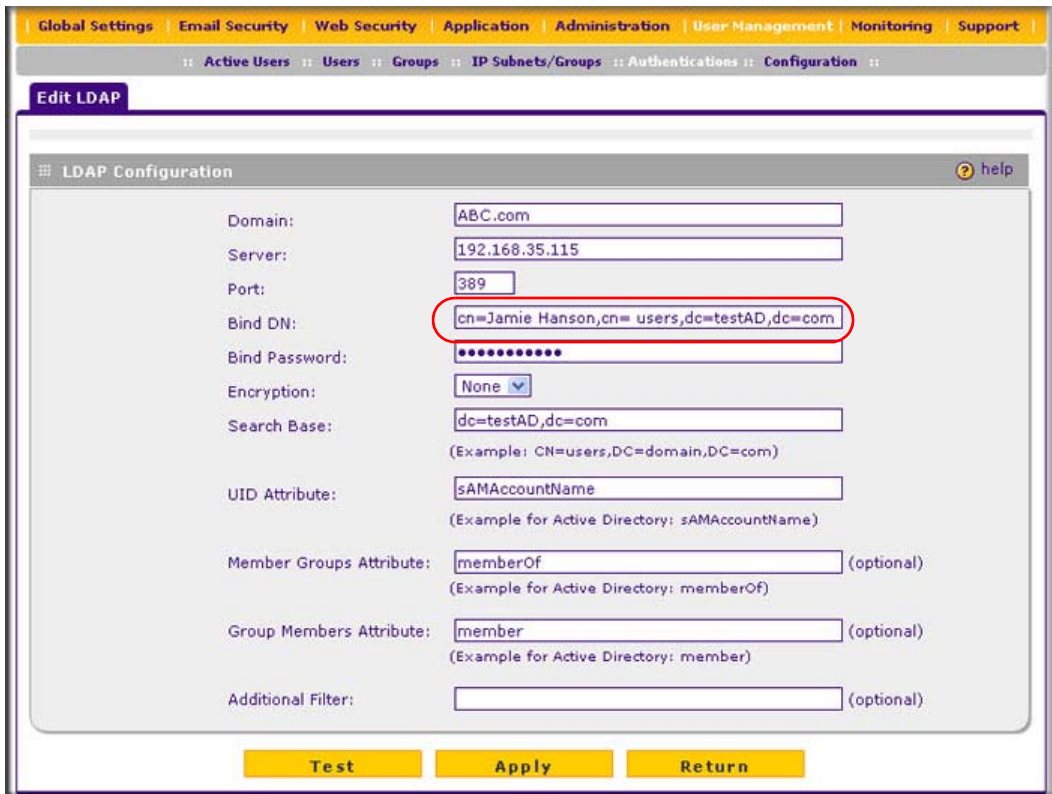


Figure 5-11

- The full name, Jamie Hanson (Figure 5-12 shows only the Bind DN field).



Figure 5-12

- The Windows account name in e-mail format such as jhanson@testAD.com (Figure 5-13 shows only the Bind DN field).



Figure 5-13

- Click **Test** to verify that the LDAP server can actually function with the bind DN that you have modified. The automated test procedure checks the connection to the LDAP server; the bind DN, and the bind password. If any settings require changes, you are notified at the end of the automated test procedure.
- Click **Apply** to save your settings.

Creating and Deleting LDAP and Active Directory Domains

To configure LDAP and Active Directory authentication:

- Select **User Management > Authentication** from the menu. The authentication submenu tabs appear with the LDAP screen in view.

The screenshot displays the configuration interface for LDAP and Active Directory domains. The top navigation bar includes tabs for Global Settings, Email Security, Web Security, Application, Administration, User Management, Monitoring, and Support. The current view is under User Management > Authentication > Configuration. The LDAP configuration screen is active, showing a list of existing LDAP servers and a form to add a new one.

List of LDAP

Domain	Server	Action
elightpostLDAP	192.168.1.50	edit delete

Add New LDAP Server:

Domain:

Server:

Port:

Bind DN:

Bind Password:

LDAP Encryption:

Search Base:
(Example: CN=users,DC=domain,DC=com)

UID Attribute:
(Example for Active Directory: sAMAccountName)

Member Groups Attribute: (optional)
(Example for Active Directory: memberOf)

Group Members Attribute: (optional)
(Example for Active Directory: member)

Additional Filter: (optional)

Test **Add**

Figure 5-14

The List of LDAP table displays the following fields:

- **Domain Name.** The name of the STM's domain to which the server has been assigned.
 - **Server.** The IP address of the LDAP or Active Directory server.
 - **Action.** The edit table button that provides access to the Edit LDAP screen and the delete table button that allows you to delete the LDAP or Active Directory server.
2. Complete the fields and make your selections from the pull-down menu as explained in [Table 5-5](#).

Table 5-5. LDAP Settings

Setting	Description
Domain	A descriptive (alphanumeric) name of the LDAP or Active Directory authentication server for identification and management purposes.
Server	The server IP address or server host name of the LDAP or Active Directory authentication server.
Port	The port number for the LDAP or Active Directory authentication server. The default port for the LDAP server is 389, which is generally the default port for TLS encryption or no encryption. When the encryption is SSL, the default port is generally 636.
Bind DN	The LDAP or Active Directory bind distinguished name (dn) that is required to access the LDAP or Active Directory authentication server. This must be a user in the LDAP or Active Directory directory that has read access to all the users that you would like to import into the STM. The Bind DN field accepts three formats: <ul style="list-style-type: none"> • A full user name. For example: a username such as Jamie Hanson. • A display name in the dn format. For example: cn=Jamie Hanson,cn=users,dc=test,dc=com. • A Windows logon account name in e-mail format. For example: jhanson@testAD.com. This last type of Bind DN can be used only for a Windows Active Directory server.
Bind Password	The authentication secret or password that is required to access the LDAP or Active Directory authentication server.
LDAP Encryption	From the pull-down menu, select the encryption type for the connection between the STM and the LDAP or Active Directory server: <ul style="list-style-type: none"> • None. The connection is not encrypted. This is the default setting. • TLS. The connection uses Transport Layer Security (TLS) encryption. • SSL. The connection uses Secure Socket Layer (SSL) encryption.
Search Base	The distinguished name (dn) at which to start the search, specified as a sequence of relative distinguished names (rdn), connected with commas and without any blank spaces. For most users, the search base is a variation of the domain name. For example, if your domain is yourcompany.com, your search base dn might be as follows: dc=yourcompany,dc=com.

Table 5-5. LDAP Settings (continued)

Setting	Description
UID Attribute	The attribute in the LDAP directory that contains the user's identifier (uid). For an Active Directory, enter sAMAccountName. For an OpenLDAP directory, enter uid.
Member Groups Attribute	This field is optional. The attribute that is used to identify the groups an entry belongs to. For an Active Directory, enter memberOf. For OpenLDAPy, you can enter a customized attribute to identify the the groups of an entry.
Group Members Attribute	This field is optional. The attribute that is used to identify the members of a group. For an Active Directory, enter: member For OpenLDAPy, you can enter a customized attribute to identify the members of a group.
Additional Filter	This field is optional. A filter that is used when searching the LDAP server for matching entries while excluding others. Use the format described by RFC 2254. The following search term examples match users only: Active Directory: objectClass=user Open LDAP: objectClass=posixAccount

- Click **Test** to verify that the LDAP server can actually function with the LDAP settings that you have specified. The automated test procedure checks the connection to the LDAP server; the bind DN, and the bind password. If any settings require changes, you are notified at the end of the automated test procedure.



Note: If the automated test procedure returns the message “LDAP server test passed but size limit exceeded,” only a limited number of entries (for example, 1000) was returned after the LDAP server was queried. To ensure that the lookup results include all users and groups, set larger values in the LDAP server. Another workaround is to use a specific search name or a name with a wildcard in the lookup process, so that the subset of the entire list is returned in the lookup result.

- Click **Apply** to save your settings. The LDAP or Active Directory domain and server are added to the List of LDAP table.

To delete a domain and server from the List of LDAP table, click the **delete** table button in the Action column for the domain and server that you want to delete.



Warning: After their sessions have expired, users can no longer log in to the STM if the domain that has been assigned to them is the domain that you deleted.

Editing LDAP and Active Directory Domains

To edit an LDAP or Active Directory domain:

1. Select **User Management** > **Authentication** from the menu. The authentication submenu tabs appear with the LDAP screen in view (see [Figure 5-14 on page 5-16](#)).
2. In the Action column of the List of LDAP table, click the **edit** table button for the domain and server that you want to edit. The Edit LDAP screen displays. This screen contains the same fields as the LDAP screen (see [Figure 5-14 on page 5-16](#)).
3. Modify the fields and make your selections from the pull-down menu as explained in [Table 5-5 on page 5-17](#).
4. Click **Test** to verify that the LDAP server can actually function with the LDAP settings that you have modified. The automated test procedure checks the connection to the LDAP server; the bind DN, and the bind password. If any settings require changes, you are notified at the end of the automated test procedure.
5. Click **Apply** to save your settings.

Creating and Deleting RADIUS Domains

To configure RADIUS authentication:

1. Select **User Management** > **Authentication** from the menu. The authentication submenu tabs appear with the LDAP screen in view.
2. Click the **RADIUS** submenu tab. The RADIUS screen displays. ([Figure 5-15 on page 5-20](#) contains one example.)

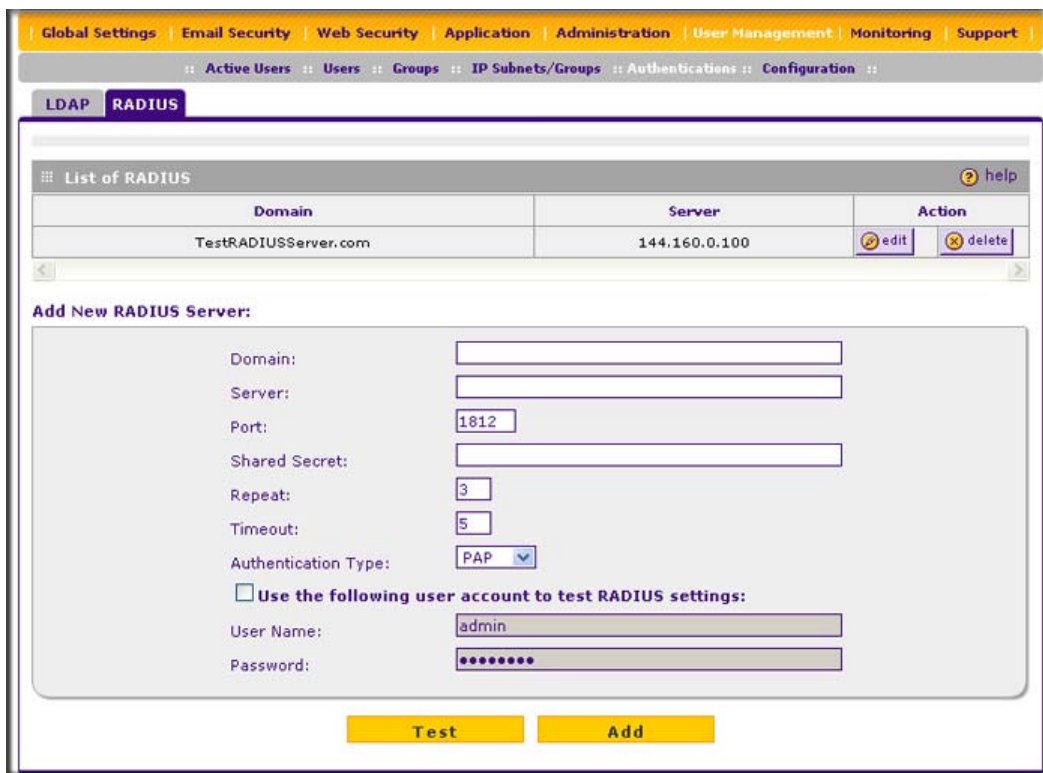


Figure 5-15

The List of RADIUS table displays the following fields:

- **Domain Name.** The name of the STM’s domain to which the server has been assigned.
- **Server.** The IP address of the RADIUS server.
- **Action.** The edit table button that provides access to the Edit RADIUS screen and the delete table button that allows you to delete the RADIUS server.

3. Complete the fields and make your selections from the pull-down menu as explained in [Table 5-6](#).

Table 5-6. RADIUS Settings

Setting	Description
Domain	A descriptive (alphanumeric) name of the RADIUS authentication server for identification and management purposes.
Server	The server IP address or server host name of the RADIUS authentication server.

Table 5-6. RADIUS Settings (continued)

Setting	Description	
Port	The port number for the RADIUS authentication server. The default port for the RADIUS server is 1812.	
Shared Secret	The shared secret (password) that is required to access the RADIUS authentication server.	
Repeat	The maximum number of times that the STM attempts to connect to the RADIUS server. The default setting is 3 times.	
Timeout	The period after which an unsuccessful connection attempt times out. The default setting is 5 seconds.	
Authentication Type	From the pull-down menu, select the encryption type for the connection between the STM and the LDAP or Active Directory server: <ul style="list-style-type: none"> • PAP. The connection uses the Password Authentication Protocol (PAP). This is the default setting. • CHAP. The connection uses the Challenge Handshake Authentication Protocol (CHAP). 	
Use the following user account to test RADIUS settings	Select this checkbox to test the RADIUS settings with the user name and password that you specify below.	
	User Name	The user name to test the RADIUS settings with.
	Password	The password to test the RADIUS settings with.

4. Click **Test** to verify that the RADIUS server can actually function with the RADIUS settings that you have specified. The automated test procedure checks the connection to the RADIUS server; the user name, and the password. If any settings require changes, you are notified at the end of the automated test procedure.
5. Click **Apply** to save your settings. The RADIUS domain and server are added to the List of RADIUS table.

To delete a domain and server from the List of RADIUS table, click the **delete** table button in the Action column for the domain and server that you want to delete.



Warning: After their sessions have expired, users can no longer log in to the STM if the domain that has been assigned to them is the domain that you deleted.

Editing RADIUS Domains and Configuring VLANs

To edit a RADIUS domain:

1. Select **User Management > Authentication** from the menu. The authentication submenu tabs appear with the LDAP screen in view.
2. Click the **RADIUS** submenu tab. The RADIUS screen displays (see [Figure 5-15](#) on page 5-20).
3. In the Action column of the List of RADIUS table, click the **edit** table button for the domain and server that you want to edit. The Edit Radius screen displays ([Figure 5-16](#) contains some examples).

The screenshot displays the 'Edit RADIUS' configuration interface. At the top, there is a navigation bar with tabs for Global Settings, Email Security, Web Security, Application, Administration, User Management, Monitoring, and Support. Below this is a breadcrumb trail: Active Users :: Users :: Groups :: IP Subnets/Groups :: Authentications :: Configuration ::. The main content area is titled 'Edit RADIUS' and contains a 'RADIUS Configuration' section with the following fields:

- Domain: TestRADIUSServer.com
- Server: 144.160.0.100
- Port: 1812
- Shared Secret: 12345678
- Repeat: 3
- Timeout: 5
- Authentication Type: PAP (dropdown menu)
- Use the following user account to test RADIUS settings:
- User Name: admin
- Password: [masked]

Below the configuration fields are three buttons: Test, Apply, and Return. At the bottom of the screen, there is a 'List of VLAN' table with the following data:

VLAN ID/Name	Brief Description	Action
TestVLAN	VLAN for test purposes	delete

Below the table is an 'Add New VLAN ID/Name' section with input fields for 'VLAN ID/Name' and 'Brief Description', and an 'Add' button with a plus icon.

Figure 5-16

4. Modify the fields and make your selections from the pull-down menu as explained in [Table 5-6 on page 5-20](#).
5. Click **Test** to verify that the RADIUS server can actually function with the RADIUS settings that you have modified. The automated test procedure checks the connection to the RADIUS server; the user name, and the password. If any settings require changes, you are notified at the end of the automated test procedure.
6. Click **Apply** to save your settings.

Creating and Deleting VLANs for Use with RADIUS Domains

After you have created a RADIUS domain by specifying a RADIUS server, you can add a virtual LAN (VLAN), and then set access exceptions for the logged-in RADIUS users (see [“Setting Web Access Exception Rules” on page 4-48](#)).

In order to use the VLAN to set access exceptions on the STM, the following is required:

- You must have defined a VLAN policy on another platform.
- You must have added users to the VLAN policy.
- The RADIUS server must contain VLAN attributes in its user information.

At the bottom of the Edit Radius screen (see [Figure 5-16 on page 5-22](#), which contains one VLAN example), the List of VLAN table displays the following fields:

- **VLAN ID/Name.** The identifier or name for the VLAN.
- **Brief Description.** An optional brief description of the VLAN.
- **Action.** The delete table button that allows you to delete the VLAN.

To add a VLAN:

1. On the Edit Radius screen, locate the Add New VLAN ID/Name section at the very bottom of the screen.
2. Specify the VLAN:
 - a. In the VLAN ID/Name field, enter the identifier or the name of the VLAN.
 - b. In the Brief Description field, enter a description of the VLAN. This field is optional.
3. Click the **add** table button. The new VLAN is added to the List of VLAN table.

To delete a user from the List of VLAN table, click the **delete** table button in the Action column for the VLAN that you want to delete.

Global User Settings

You can globally set the user session settings for authenticated users. These settings include the session expiration period, the allowed session idle time, and the default domain that is presented to the users. To specify the global user configuration settings:

1. Select **User Management > Configuration** from the menu. The Configuration screen displays.

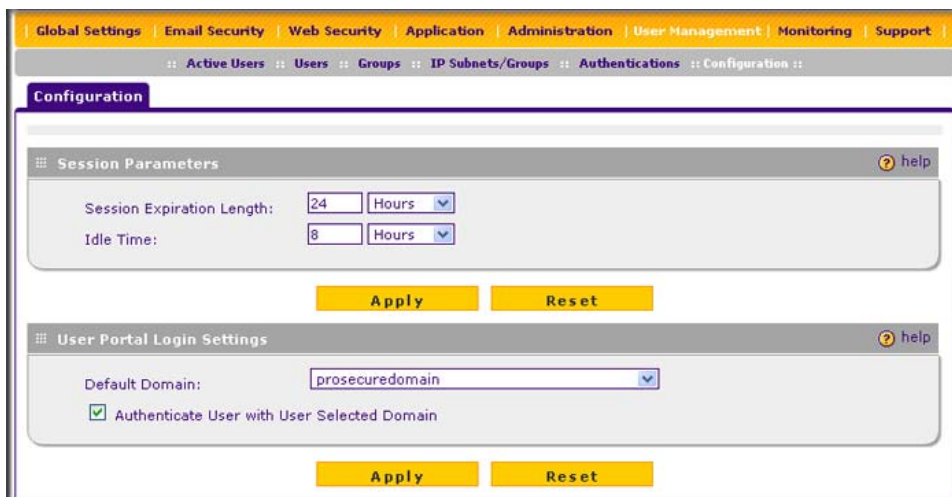



Figure 5-17

2. Locate the Sessions Parameters section on screen, and specify the session settings:
 - **Session Expiration Length.** The period after which a session expires and a user must log in again. This setting applies to all users. From the pull-down menu, select either **Minutes** or **Hours**. Then, in the field to the left of the pull-down menu, enter a number for the minutes or hours. The session expiration length cannot exceed the idle time period.

	Note: To set the time-out period for the Web Management Interface, see “Changing Administrative Passwords and Timeouts” on page 3-9.
---	---

- **Idle Time.** The period after which an idle connection is terminated and a user must log in again. This setting applies to all users. From the pull-down menu, select either **Minutes** or **Hours**. Then, in the field to the left of the pull-down menu, enter a number for the minutes or hours. The idle time period cannot exceed the session expiration length.

3. Click **Apply** to save the session settings.
4. Locate the Users Portal Login Settings section on screen, and specify the default domain settings:
 - From the **Default Domain** pull-down menu, select a domain that is presented as the default domain on the User Portal Login screen. The default domain that is presented is `prosecuredomain`. Users can still select another domain (if there are other domains configured on the STM) from the pull-down menu on the User Portal Login screen.
 - Select the **Authenticate User with User Selected Domain** checkbox to limit the authentication to the default domain that you select. If you do not select this checkbox, the STM attempts to authenticate users through all the domains that are listed in the pull-down menu on the User Portal Login screen; when authentication through one domain fails, the STM attempts authentication through another domain.
5. Click **Apply** to save the default domain settings.

Viewing and Logging Out Active Users

A users with administrative privileges can view the active users and log out selected or all active users. To log out all active users:

1. Select **User Management > Active Users** from the menu. The Active Users screen displays.

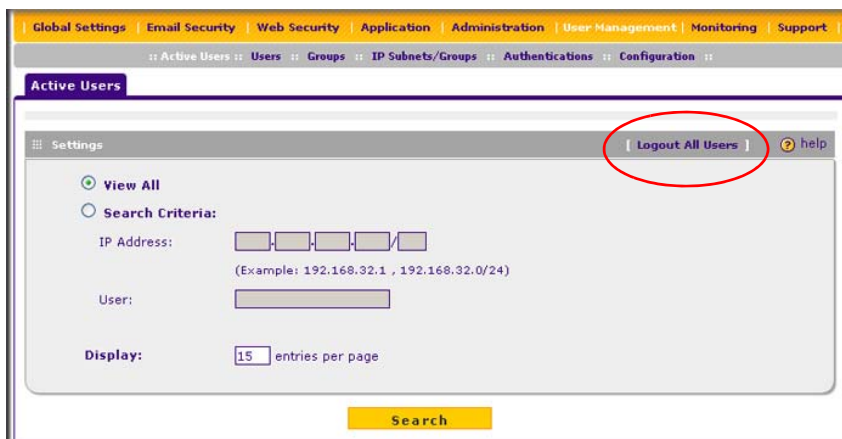


Figure 5-18

2. Click the **Logout All Users** button in the gray Settings bar at the top of the Active Users screen.

To view all or selected users:

1. On the Active Users screen (see [Figure 5-18 on page 5-25](#)), select one of the following radio buttons:
 - **View All.** This selection returns all active users after you have clicked the Search button.
 - **Search Criteria.** This selection lets you enter the following search criteria so that only selected users are returned after you have clicked the Search button.

Either use the IP address or User field, but not both:

- **IP Address.** Enter an IP address or an IP address and subnet mask in CIDR notation (for example, /024).
 - **User.** Enter a domain and user name in the domain:name format (for example, prosecuredomain:JohnP).
2. In the Display field, enter a number to specify how many entries per page the search result screen returns.
 3. Click **Search**. The search result screen displays ([Figure 5-19](#) contains an example).



Figure 5-19

The List of Users table displays the following fields:

- **IP Address.** The IP address that is associated with the user.
- **User.** The domain that is associated with the user and the user name.
- **Group.** The group to which the user belongs, if any.
- **Last Seen.** The most recent time that scanned traffic associated with the user (that is, IP address) passed through the STM.

To log out selected active users:

1. On the search result screen select the checkboxes to the left of the users that you want to log out.
2. Click **Logout**.

Chapter 6

Monitoring System Access and Performance

This chapter describes the system monitoring features of the STM. You can be alerted to important events such as attacks and login failures. You can also view the system status and real-time traffic and security information. In addition, the diagnostics utilities are described.



Note: All log and report functions that are part of the Logs & Reports configuration menu and some of the functions that are part of the Diagnostics configuration menu require that you configure the e-mail notification server—see [“Configuring the E-mail Notification Server”](#) on page 6-2.

This chapter contains the following sections:

- [“Configuring Logging, Alerts, and Event Notifications”](#) on this page.
- [“Monitoring Real-Time Traffic, Security, Statistics, and Web Usage”](#) on page 6-11.
- [“Viewing System Status”](#) on page 6-19.
- [“Querying Logs and Generating Reports”](#) on page 6-22.
- [“Viewing and Managing the Quarantine Files”](#) on page 6-33.
- [“Using Diagnostics Utilities”](#) on page 6-40.

Configuring Logging, Alerts, and Event Notifications

You can configure the STM to e-mail logs and alerts to a specified e-mail address. For example, the STM can e-mail security-related events such as malware incidents, infected clients, and failed authentications. By default, the STM logs content filtering events such as attempts to access blocked sites and URLs, unwanted e-mail content, spam attempts, and many other types of events.

To receive the logs in an e-mail message, the STM’s notification server must be configured and e-mail notification must be enabled. If the notification server is not configured or e-mail notification is disabled, you can still query the logs and generate log reports to view on the Web Management Interface screen or to save in CSV format.

For more information about logs, see [“Querying Logs and Generating Reports”](#) on page 6-22.

Configuring the E-mail Notification Server

If you have used the Setup Wizard, you might have already configured the e-mail notification server; the E-mail Notification Server screen allows you to modify these settings.

The STM can automatically send information such as notifications and reports to an administrator. You must configure the necessary information for sending e mail, such as the administrator's e-mail address, the e-mail server, user name, and password.

To configure the e-mail notification server:

1. Select **Global Settings > Email Notification Server** from the menu. The Email Notification Server screen displays (Figure 6-1 contains some examples).

The screenshot shows the 'Email Notification Server' configuration page. At the top, there is a navigation bar with tabs: Global Settings, Email Security, Web Security, Application, Administration, User Management, Monitoring, and Support. Below this is a breadcrumb trail: Network Settings :: HTTP Proxy :: Scanning Exclusions :: Exceptions :: Email Notification Server :: Quarantine :: Setup Wizard. The main content area is titled 'Email Notification Server' and contains the following fields:

- Show as Mail Sender:
- Send Notifications to: (Example: admin@yourdomain.com)
- SMTP Server: :
- Mail Server Requires Authentication
- User Name:
- Password:

At the bottom of the form are two buttons: 'Apply' and 'Reset'.

Figure 6-1

2. Complete the fields, select the radio button and checkboxes, and make your selections from the pull-down menus as explained in Table 6-1.

Table 6-1. E-mail Notification Settings

Setting	Description (or Subfield and Description)
Show as Mail sender	A descriptive name of the sender for e-mail identification purposes. For example, enter stm600notification@netgear.com.
Send Notifications to	The e-mail address to which the notifications should be sent. Typically, this is the e-mail address of a user with administrative privileges.

Table 6-1. E-mail Notification Settings (continued)

Setting	Description (or Subfield and Description)	
SMTP server	The IP address and port number or Internet name and port number of your ISP's outgoing e-mail SMTP server. The default port number is 25. Note: If you leave this field blank, the STM cannot send e-mail notifications.	
Mail Server Requires Authentication	If the SMTP server requires authentication, select the Mail Server Requires Authentication checkbox and enter the following settings:	
	User Name	The user name for SMTP server authentication.
	Password	The password for SMTP server authentication.

3. Click **Apply** to save your settings.

Configuring and Activating System, E-mail, and Syslog Logs

You can configure the STM to log system events such as a change of time by an NTP server, secure login attempts, restarts, and other events. You can also send logs to the administrator or schedule logs to be sent to the administrator or to a syslog server on the network. In addition, the Email and Syslog screen provides the option to selectively clear logs. Because this large screen has three sections, each with its own Apply button, this screen is presented in this manual in three figures ([Figure 6-2 on page 6-4](#), [Figure 6-3 on page 6-6](#), and [Figure 6-4 on page 6-8](#)).

E-mailing Logs

To enable and configure logs to be sent to an e-mail address:

1. Select **Monitoring > Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view (see [Figure 6-2 on page 6-4](#), [Figure 6-4 on page 6-8](#), and [Figure 6-4 on page 6-8](#)).
2. Locate the Email Logs to Administrator section on the screen.

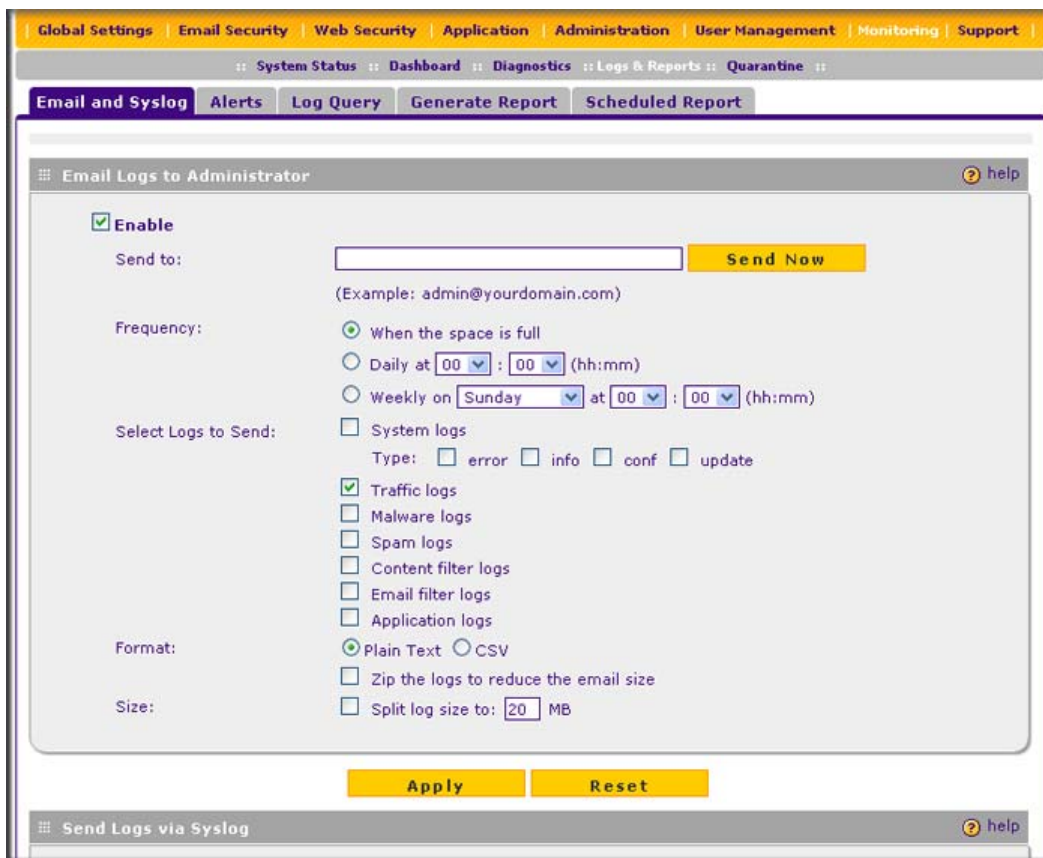


Figure 6-2 [Email and Syslog, screen 1 of 3]

3. Select the **Enable** checkbox to enable the STM to send logs to an e-mail address.
4. Complete the fields, select the radio button and checkboxes, and make your selections from the pull-down menus as explained in [Table 6-2](#).

Table 6-2. E-mail Logs Settings

Setting	Description (or Subfield and Description)
Send to	The e-mail address of the recipient of the log file. This is normally a user with administrative privileges. You enter up to three e-mail address, separated by commas. Click Send Now to immediately send the logs that you first must have specified below.

Table 6-2. E-mail Logs Settings (continued)

Setting	Description (or Subfield and Description)
Frequency	Select a radio button to specify how often the log file is sent: <ul style="list-style-type: none"> • When the space is full. Logs are sent when the storage space that is assigned to the logs is full. • Daily. Logs are sent daily at the time that you specify from the pull-down menus (hours and minutes). • Weekly. Logs are sent weekly at the day and time that you specify from the pull-down menus (weekday, hours, and minutes).
Select Logs to Send	Select the checkboxes to specify which logs are sent via e-mail: <ul style="list-style-type: none"> • System logs. The system event logs that include all system errors, informational messages, configuration changes, and system software updates. • Traffic logs. All scanned incoming and outgoing traffic. • Malware logs. All intercepted viruses and spyware. • Spam logs. All intercepted spam, including spam that was detected through the blacklist, real-time blacklist, and Distributed Spam Analysis. • Content filter logs. All Web sites, URLs, and FTP sites that are intercepted because of Web category, blacklist, file type, or size limit violations. • Email filter logs. All e-mails that are intercepted because of keyword, file type, file name, password, or size limit violations. • Application logs. All intercepted application access violations.
	Select the types of system logs that are sent via e-mail: <ul style="list-style-type: none"> • error. All system errors. • info. All informational messages. • conf. All configuration changes. • update. All system software updates.
Format	Select a radio button to specify the format in which the log file is sent: <ul style="list-style-type: none"> • Plain text. The log file is sent as a plain text file. • CSV. The log file is sent as a comma separated values (CSV) file.
	Select the Zip the logs to save space checkbox to enable the STM to compress the log file.
Size	Select the Split logs size to checkbox to break up the log file into smaller files, and specify the maximum size of each file in MB. The default setting is 20 MB.

5. Click **Apply** to save your settings.

Sending Log to a Syslog Servers

To enable and configure logs to be sent to a syslog server:

1. Select **Monitoring > Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view (see [Figure 6-3 on page 6-6](#)).
2. Locate the Send Logs via Syslog section on the screen.

Figure 6-3 [Email and Syslog, screen 2 of 3]

4. Select the **Enable** checkbox to enable the STM to send logs to a syslog server.
5. Complete the fields, select the checkboxes, and make your selections from the pull-down menus as explained in [Table 6-3](#).

Table 6-3. Syslog Settings

Setting	Description (or Subfield and Description)
IP Address	The IP address of the syslog server.
Port	The port number that the syslog server uses to receive logs. The default port number is 514.
Logs	<p>Select the checkboxes to specify which logs are sent to the syslog server:</p> <ul style="list-style-type: none"> • System logs. The system event logs that include all system errors, informational messages, configuration changes, and system software updates. • Traffic logs. All scanned incoming and outgoing traffic. • Malware logs. All intercepted viruses and spyware. • Spam logs. All intercepted spam, including spam that was detected through the blacklist, real-time blacklist, and Distributed Spam Analysis. • Content filter logs. All Web sites, URLs, and FTP sites that are intercepted because of Web category, blacklist, file type, or size limit violations. • Email filter logs. All e-mails that are intercepted because of keyword, file type, file name, password, or size limit violations. • Application logs. All intercepted application access violations.

Table 6-3. Syslog Settings (continued)

Setting	Description (or Subfield and Description)
Facility	<p>The facility indicates from which internal part of the STM the log message originates. For each log that you have selected to be sent to the syslog server (see above), select one of the following facilities from the pull-down menu:</p> <ul style="list-style-type: none"> • auth. security and authorization log messages. • authpriv. Security and authorization log messages for sensitive information. • cron. Clock daemon log messages. • daemon. Other daemon log messages. • ftp. FTP log messages. • kern. Kernel log messages. • local0 through local7. Locally defined log messages (1 through 7). • lpr. Line printer subsystem log messages. • mail. Mail subsystem log messages. • news. Usenet news subsystem log messages. • syslog. Log messages that are generated internally by the syslog server (syslogd). • user. Generic user-level log messages. • uucp. Unix-Unix copy (UUCP) subsystem log messages.
Priority	<p>For each log that you have selected to be sent to the syslog server (see above), select one of the following severities from the pull-down menu:</p> <ul style="list-style-type: none"> • emerg. The STM is unusable. • alert. An action must be taken immediately. • crit. There are critical conditions. • err. There are error conditions. • warning. There are warning conditions. • notice. There are normal but significant conditions. • info. Informational messages. • debug. Debug-level messages. <p>Note: All the logs with a severity that is equal to and above the severity that you specify are logged on the specified syslog server. For example, if you select crit as the severity, then the logs with the severities crit, alert, and emerg are logged.</p>

6. Click **Apply** to save your settings.

Clearing Logs

1. Select **Monitoring > Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view (see [Figure 6-4 on page 6-8](#)).

2. Locate the Clear the Following Log Information section at the bottom of the screen.

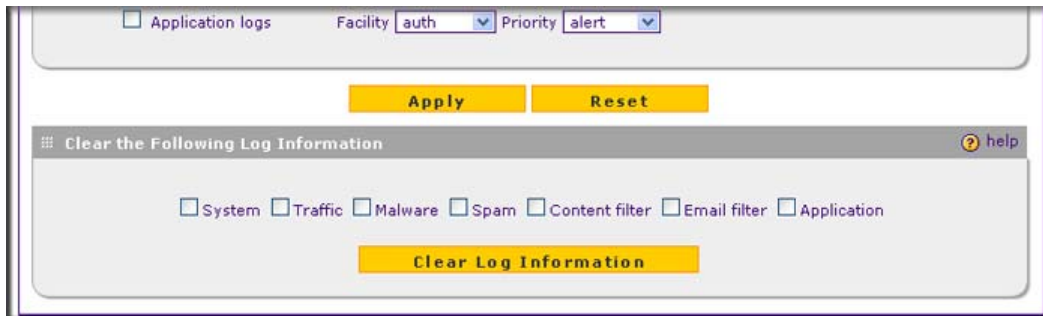


Figure 6-4 [Email and Syslog, screen 3 of 3]

3. Select the checkboxes to specify which logs are cleared:
 - **System.** The system event logs are cleared.
 - **Traffic.** The logs with scanned incoming and outgoing traffic are cleared.
 - **Malware.** The logs with intercepted viruses and spyware are cleared.
 - **Spam.** The logs with intercepted spam are cleared.
 - **Content filter.** The logs with intercepted Web sites, URLs, and FTP sites are cleared.
 - **Email filter.** The logs with intercepted e-mails are cleared.
 - **Application.** The logs with intercepted applications are cleared.
4. Click **Clear Log Information**.

Configuring Alerts

You can configure the STM to send an e-mail alert when a failure, license expiration, or malware attack or outbreak occurs. Four types of alerts are supported:

- **Update Failure Alert.** Sent when an attempt to update any component such as a pattern file or scan engine firmware fails.
- **License Expiration Alerts.** Sent when when a license is about to expire and then again when a license has expired.
- **Malware Alert.** Sent when the STM detects malware threats.
- **Malware Outbreak Alert.** Sent when the malware outbreak criteria that you have configured are reached or exceeded. Outbreak criteria are based on the number of malware threats detected within a specified period of time.

To configure and activate the e-mail alerts:

1. Select **Monitoring > Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Alerts** submenu tab. The Alerts screen displays.

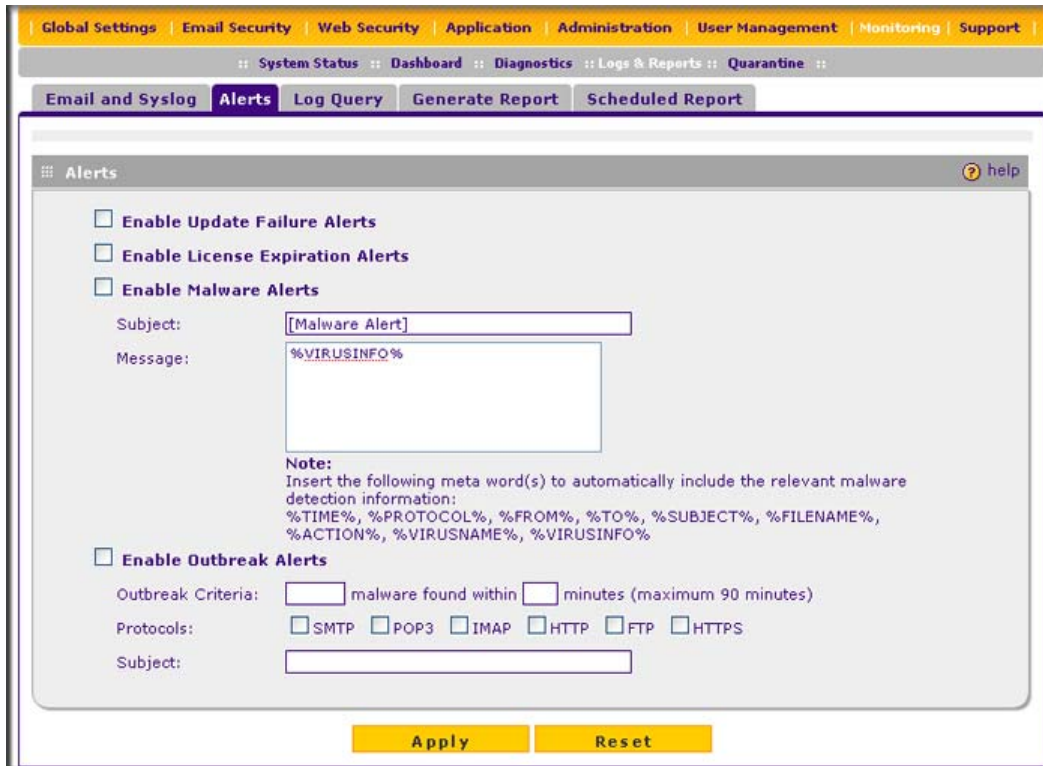


Figure 6-5

3. Select the checkboxes and complete the fields as explained in [Table 6-4](#).

Table 6-4. Alerts Settings

Setting	Description (or Subfield and Description)
Enable Update Failure Alerts	Select this checkbox to enable update failure alerts.
Enable License Expiration Alerts	Select this checkbox to enable update license expiration alerts.

Table 6-4. Alerts Settings (continued)

Setting	Description (or Subfield and Description)	
Enable Malware Alerts	Select this checkbox to enable malware alerts, and configure the Subject and Message fields.	
	Subject	Enter the subject line for the e-mail alert. The default text is “[Malware alert]”.
	Message	Enter the content for the e-mail alert. The default text is %VIRUSINFO%, which is the meta word that enables the STM to insert the proper malware threat information Note: In addition to the %VIRUSINFO% meta word, you can insert the following meta words in your customized message: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%.
Enable Malware Outbreak Alerts	Select this checkbox to enable malware outbreak alerts, and configure the Outbreak Criteria, Protocol, and Subject fields.	
	Outbreak Criteria	To define a malware outbreak, specify the following fields: <ul style="list-style-type: none"> • malware found within. The number of malware incidents that are detected. • minutes (maximum 90 minutes). The period in which the specified number of malware incidents are detected. Note: When the specified number of detected malware incidents is reached within the time threshold, the STM sends a malware outbreak alert.
	Protocol	Select the checkbox or checkboxes to specify the protocols (SMTP, POP3, IMAP, HTTP, FTP, and HTTPS) for which malware incidents are detected.
	Subject	Enter the subject line for the e-mail alert.

- Click **Apply** to save your settings.

Monitoring Real-Time Traffic, Security, Statistics, and Web Usage

You can monitor the real-time traffic, security events, and statistics from the Dashboard screen. The Web Usage screen displays which hosts on your network are consuming the most resources.

Understanding the Information on the Dashboard Screen

When you start up the STM, the default screen that displays is the Dashboard screen, which lets you monitor the following items:

- CPU, memory, and hard disk status.
- The number of active connections per protocol.
- The total malware threats and the malware threats over the last seven days.
- Total scanned services traffic over the last seven days.
- Statistics for the most recent five and top five malware threats detected, applications blocked, Web categories blocked, and spam e-mails blocked.
- The real-time security scanning status with detected network traffic, detected network threats, and service statistics for the six supported protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP).
- Interface statistics.

To display the Dashboard screen, select **Monitoring > Dashboard** from the menu. The dashboard submenu tabs appear with the Dashboard screen in view. Because of the size of this screen, it is divided and presented in this manual in three figures ([Figure 6-6 on page 6-12](#), [Figure 6-7 on page 6-14](#), and [Figure 6-8 on page 6-16](#)), each with its own table that explains the fields.

Except for setting the poll interval and clearing the statistics, you cannot configure the fields on the Dashboard screen. Any changes must be made on other screens.

To set the poll interval:

1. Click the **stop** button.
2. From the Poll Interval pull-down menu, select a new interval (the minimum is 5 seconds, the maximum is 5 minutes).
3. Click the **set interval** button.

To clear the statistics, click **Clear statistics**.

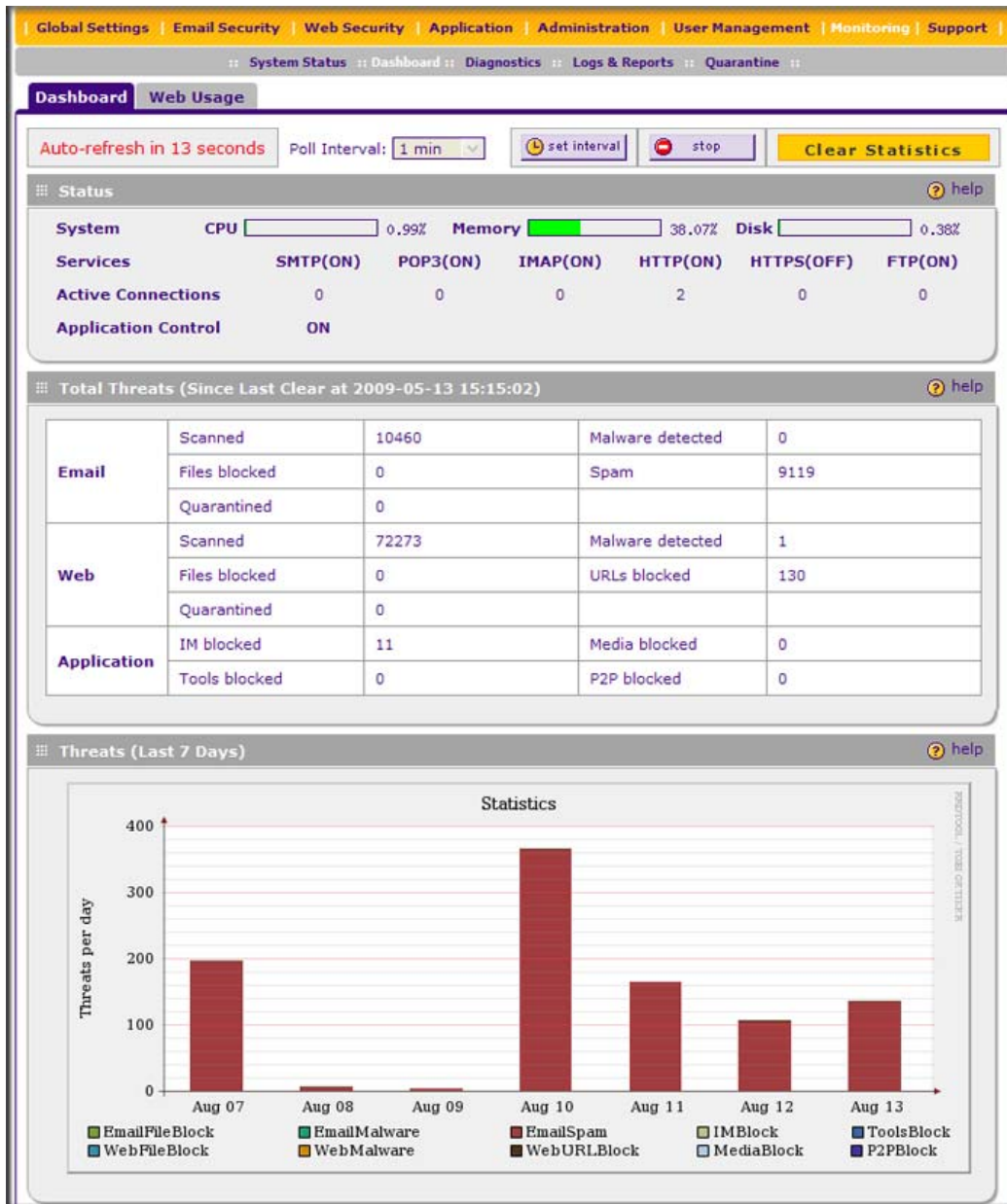


Figure 6-6 [Dashboard, screen 1 of 3]

Table 6-5 on page 6-13 explains the fields of the Status, Total Threats, Threats (Last 7 Days) sections of the Dashboard screen.

Table 6-5. Dashboard: Status, Total Threats, and Threats (Last 7 Days) formation

Item	Description
Status	
System	The current CPU, memory, and hard disk usage. When usage is within safe limits, the status bars show green.
Services	The protocols that are being scanned for malware threats. (ON, OFF, or HALT stated next to the protocol) and the number of active connections for each protocol. ON indicates that protocol is scanned. OFF indicates that the protocol is not scanned. HALT indicates that you enabled protocol scanning but the protection license has expired.
Active Connections	The number of active connection per protocol.
Application Control	ON indicates that application control is enabled; OFF indicates that application control is disabled. HALT indicates that you enabled application control but the protection license has expired. To configure application control, see “Configuring Application Control” on page 4-44 .
Total Threats (Since Last Clear)	
Email	Displays the total number of: <ul style="list-style-type: none"> • Scanned (e-mails). • Files blocked (to configure, see “E-mail Content Filtering” on page 4-11). • Quarantined (to configure, see “E-mail Content Filtering” on page 4-11). • Malware detected (to configure, see “Customizing E-mail Anti-Virus Settings” on page 4-5). • Spam (to configure, see “Protecting Against E-mail Spam” on page 4-14).
Web	Displays the total number of: <ul style="list-style-type: none"> • Scanned (files). • Files blocked (to configure, see “Configuring Web Content Filtering” on page 4-26). • Quarantined (to configure, see “Configuring Web Content Filtering” on page 4-26). • Malware detected (to configure, see “Configuring Web Malware Scans” on page 4-24). • URLs blocked (to configure, see “Configuring Web URL Filtering” on page 4-32).
Application	Displays the total number of: <ul style="list-style-type: none"> • IM blocked. • Tools blocked. • Media blocked. • P2P blocked. <p>Note: To configure these applications, see “Configuring Application Control” on page 4-44</p>

Table 6-5. Dashboard: Status, Total Threats, and Threats (Last 7 Days) formation

Item	Description
Threats (Last 7 Days)	
This is a graphic that shows the relative number of threats and access violations over the last week, using different colors for the various applications:	
Note: IMBlock stands for instant messaging applications blocked; P2PBlock stands for peer-to-peer applications blocked.	
Note: Figure 6-6 on page 6-12 shows only graphics for blocked e-mail spam.	

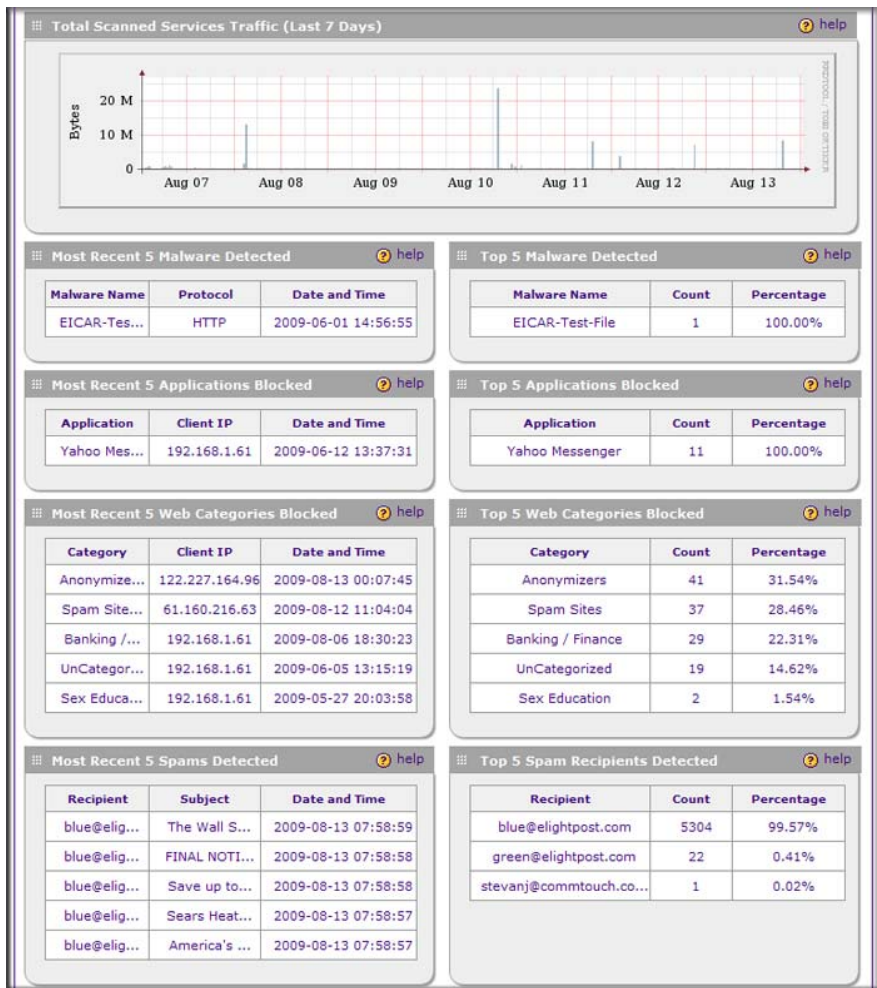


Figure 6-7 [Dashboard, screen 2 of 3]

Table 6-6 explains the fields of the Total Scanned Services Traffic, Most Recent 5 and Top 5 sections of the Dashboard screen.

Table 6-6. Dashboard: Total Scanned Services Traffic and Most Recent 5 and Top 5 Information

Item	Description	
Total Scanned Services Traffic (Last 7 Days)		
This is a graphic that shows the relative number of traffic in bytes over the last week.		
Category	Most Recent 5 Description	Top 5 Description
Malware	<ul style="list-style-type: none"> • Malware Name. The name of the malware threat. • Protocol. The protocol in which the malware threat was detected. • Date and Time. The date and time that the malware threat was detected. 	<ul style="list-style-type: none"> • Malware Name. The name of the malware threat. • Count. The number of times that the malware threat was detected. • Percentage. The percentage that the malware threat represents in relation to the total number of detected malware threats.
Application	<ul style="list-style-type: none"> • Application. The name of the application that was blocked. • Client IP. The client IP address from which the application request came. • Date and Time. The date and time that the application request was blocked. 	<ul style="list-style-type: none"> • Application. The name of the application that was blocked. • Count. The total number of user requests for the blocked application. • Percentage. The percentage that the application represents in relation to the total number of detected application requests.
Web	<ul style="list-style-type: none"> • Category. The Web category that was blocked. • Note: For more information about Web categories, see “Configuring Web Content Filtering” on page 4-26. • Client IP. The client IP address from which the Web request came. • Date and Time. The date and time that the Web request was blocked. 	<ul style="list-style-type: none"> • Category. The Web category that was blocked. • Note: For more information about Web categories, see “Configuring Web Content Filtering” on page 4-26. • Count. The total number of Web requests for the blocked Web category. • Percentage. The percentage that the Web category represents in relation to the total number of blocked Web categories.
Spam	<ul style="list-style-type: none"> • Recipient. The intended recipient of the spam message. • Subject. The e-mail subject line in the spam message. • Date and Time. The date and time that the spam message was detected. 	<ul style="list-style-type: none"> • Recipient. The intended recipient of the spam message. • Count. The number of spam messages for the intended recipient . • Percentage. The percentage that the spam message represents in relation to the total number of detected spam messages.

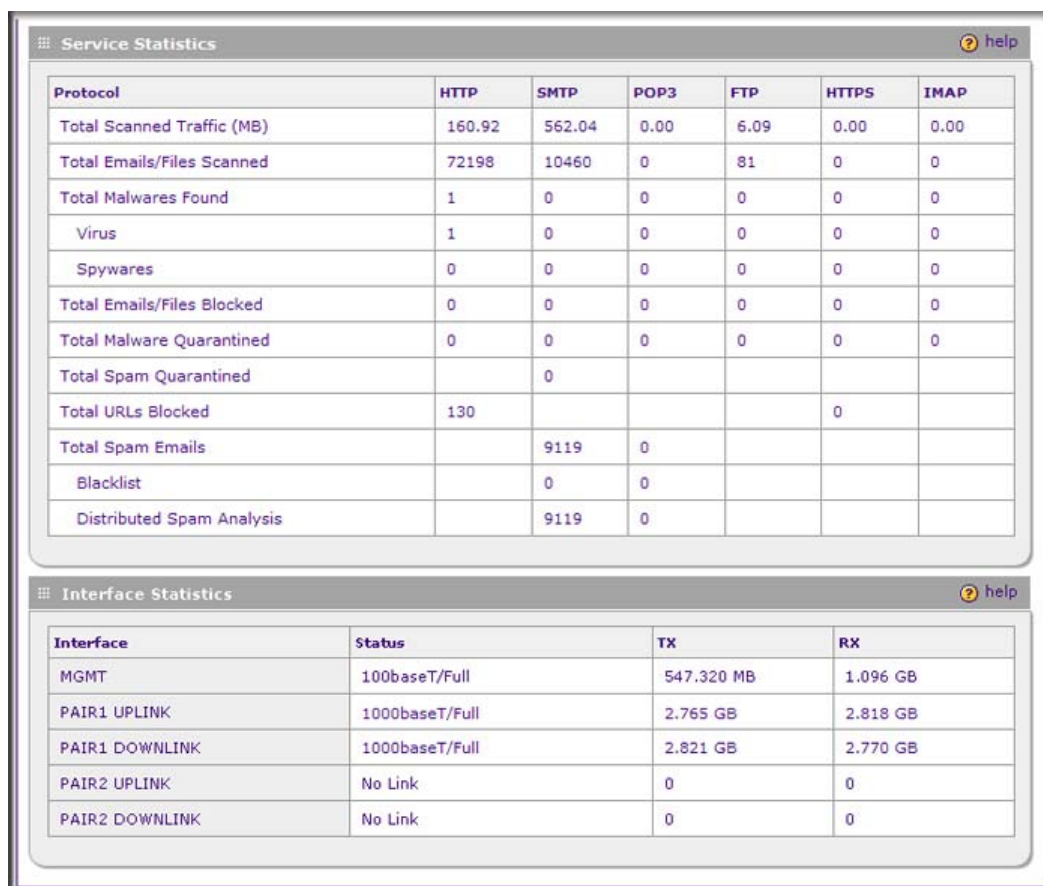


Figure 6-8 [Dashboard, screen 3 of 3]



Note: Figure 6-8 shows the Interface Statistics section of the STM600. The STM300 and STM150 have different interfaces (see [Table 6-7 on page 6-17](#)).

[Table 6-7 on page 6-17](#) explains the fields of the Service Statistics and Interface Statistics sections of the Dashboard screen.

Table 6-7. Dashboard: Service Statistics and Interface Statistics Information

Item	Description	
Service Statistics		
For each of the six supported protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP), this section provides the following statistics:		
Total Scanned Traffic (MB)	The total quantity of scanned traffic in MB.	
Total Emails/Files Scanned	The total number of scanned e-mails and files.	
Total Malwares Found	The total number of detected malware threats.	
	Virus	The total number of detected viruses
	Spyware	The total number of detected spyware.
Total Emails/Files Blocked	The total number of blocked e-mails and files.	
Total Malware Quarantined	The total number of detected malware threats that were placed in quarantine.	
Total Spam Quarantined	The total number of spam messages that were placed in quarantine. Note: These statistics are applicable only to SMTP.	
Total URLs Blocked	The total number of URL requests that were blocked. Note: These statistics are applicable only to HTTP and HTTPS.	
Total Spam Emails	The total number of spam e-mails that were detected. Note: These statistics are applicable only to SMTP and POP3.	
	Blacklist	The total number of e-mails that were detected through the spam blacklist and the real-time blacklist (see “Setting Up the Whitelist and Blacklist” on page 4-15 and “Configuring the Real-time Blacklist” on page 4-17).
	Distributed Spam Analysis	The total number of spam messages that were detected through Distributed Spam Analysis (see “Configuring Distributed Spam Analysis” on page 4-19).
Interface Statistics		
STM600: MGMT (Management), PAIR1 UPLINK, PAIR1 DOWNLINK, PAIR2 UPLINK, PAIR2 DOWNLINK. STM300: MGMT, UPLINK, DOWNLINK. STM150: LAN1, LAN2, LAN3, LAN4, WAN.		
For each interface the following statistics are displayed:		
Status	10BaseT Half duplex, 10BaseT Full duplex, 100BaseT Half duplex, 100BaseT Full duplex, or No Link.	
TX	The number of transmitted packets in KB, MB, or GB (as stated on the screen).	
RX	The number of received packets in KB, MB, or GB (as stated on the screen).	

Monitoring Web Usage

The Web Usage screen shows you how the STM's Web resources are being used. You can see, for example, which host on the STM uses most resources.

To view the STM's Web usage:

1. Select **Monitoring** > **Dashboard** from the menu. The dashboard submenu tabs appear with the Dashboard screen in view.
2. Click the **Web Usage** submenu tab. The Web Usage screen displays.

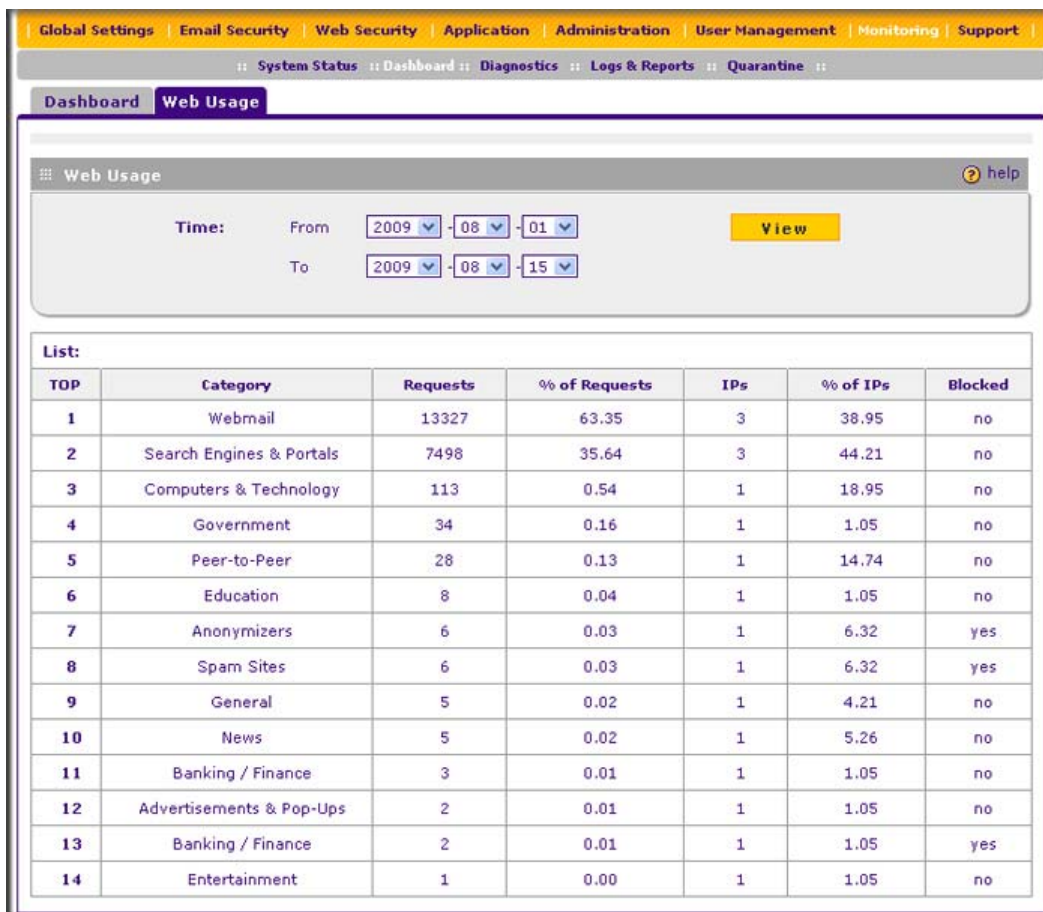


Figure 6-9

3. Use the **From** pull-down menu to select the start date of the Web usage report (year, month, date) and the **To** pull-down menu to select the end date of the report (year, month, date).
4. Click **View**. The STM generates a Web usage report.

The Web usage reports shows the following columns:

- **TOP**. The Web usage ranking.
- **Category**. The Web content filtering category.
- **Requests**. The number of requests for the category.
- **% of Requests**. The percentage of requests for the category in relation to the total number of Web requests.
- **IPs**. The number of IP addresses that request the category.
- **% of IPs**. The percentage of IP addresses that request the category in relation to the total number of IP addresses.
- **Blocked**. Whether or not the category is blocked by the STM.

Viewing System Status

The System Status screen provides real-time information about the following components of the STM:

- Firmware versions and update information of the STM, software versions and update information of the components, license expiration dates for each type of license, and hardware serial number.
- Management interface information.
- MAC addresses for the STM's interfaces.

To view the System Status screen click **Monitoring > System Status**. [Figure 6-10 on page 6-20](#) displays the System Status screen of the STM600. The Interfaces section of the System Status screen differs for STM300 and STM150 (see the explanation in [Table 6-8 on page 6-21](#)).

System Status

System Information help

Component	Current Version	Last Update
Software	V2.0.0-23	2009-08-12
Scan Engine	V5.5.4.171	2009-05-05
Pattern File	200908160000	2009-08-16
OS	V1.1.0.31	2009-06-05

Hardware Serial Number: 24V192XX00027

License Key	License Type	Expiration Date
NG2002-1234-A111-B111-2345-AA22-3456-1AB2-000C	Web Protection	2010-07-21
NG2001-9876-B222-C333-8765-BB33-7654-2FF3-111D	Email Protection	2010-07-21
NG2000-6789-C333-D444-6543-CC44-4567-3DD2-222E	Support & Maintenance	2010-07-21

Upon license expiration, the LED blinks to remind you to renew. Press the following button to stop the LED from blinking: **Stop LED Blinking**

Management Interface Information help

System Name:	STM600
IP Address:	192.168.1.161
Subnet Mask:	255.255.255.0
Gateway IP Address:	192.168.1.254
Primary DNS:	192.168.1.254
Secondary DNS:	4.2.2.2

Interfaces help

Interface	MAC Address
MGMT	00:90:0B:10:D3:29
PAIR1 DOWNLINK	00:90:0B:10:D3:2B
PAIR1 UPLINK	00:90:0B:10:D3:2A
PAIR2 DOWNLINK	00:90:0B:10:D4:97
PAIR2 UPLINK	00:90:0B:10:D4:96

Figure 6-10

Table 6-8 on page 6-21 explains the fields of the System Information, Management Interface Information, and Interfaces sections of the System Status screen.

Table 6-8. System Status Information

Setting	Description
System Information	
Firmware Information	The current version and most recent update (that is, the most recently downloaded version) for the software, scan engine, pattern file, and operating system (OS).
Hardware Serial Number	The hardware serial number of the STM.
License Expiration Date	<p>The license keys and the expiration dates for the e-mail protection, Web protection, and maintenance and support licenses.</p> <p>Note: When a license has expired, the license expiration date is displayed in red font.</p> <p>When a license expires, a LED (see below) on the front panel of the STM blinks continuously to remind you to renew the license. To stop the blinking of the LED, click Stop LED Blinking.</p> <p>On the STM150: The Test LED blinks when a license expires. On the STM300 and STM600: The Status LED blinks when a license expires.</p>
Management Interface Information	
System Name	These fields are self-explanatory. You can configure these fields on the Network Settings screen (see "Configuring Network Settings" on page 3-1).
IP Address	
Subnet Mask	
Gateway IP Address	
Primary DNS	
Secondary DNS	
Interfaces	
<p>The MAC addresses of the STM's interfaces. (Figure 6-10 on page 6-20 displays the System Status screen for the STM600.)</p> <p>STM600: MGMT (Management), PAIR1 DOWNLINK, PAIR1 UPLINK, PAIR2 DOWNLINK, PAIR2 UPLINK. STM300: MGMT, DOWNLINK, UPLINK. STM150: LAN, WAN. (The four LAN interfaces share a single MAC address.)</p>	

Querying Logs and Generating Reports

The extensive logging and reporting functions of the STM let you perform the following tasks that help you to monitor the protection of the network and the performance of the STM:

- Querying and downloading logs
- Generating and downloading e-mail, Web, and system reports
- Scheduling automatic e-mail, Web, and system reports, and e-mailing these reports to specified recipients.

For information about e-mailing logs and sending logs to a syslog server, see [“Configuring and Activating System, E-mail, and Syslog Logs”](#) on page 6-3.

Querying the Logs

The STM generates logs that provide detailed information about malware threats and traffic activities on the network. You can search and view these logs through the Web Management Interface or save the log records in CSV or HTML format and download them to a computer (the downloading option is not available for all logs). You can also specify how many entries are displayed per page (the default setting is 15 entries).

The STM provides eight types of logs:

- **Traffic.** All scanned incoming and outgoing traffic.
- **Virus.** All intercepted viruses.
- **Spyware.** All intercepted spyware.
- **Spam.** All intercepted spam, including spam that was detected through the blacklist, real-time blacklist, and Distributed Spam Analysis.
- **Email filters.** All e-mails that are intercepted because of keyword, file type, file name, password, or size limit violations.
- **Content filters.** All Web sites, URLs, and FTP sites that are intercepted because of Web category, blacklist, file type, or size limit violations.
- **System.** The system event logs that include all system errors, informational messages, configuration changes, and system software updates.
- **Application.** All intercepted application access violations.

You can query and generate each type of log separately and filter the information based on a number of criteria. For example, you can filter the virus logs using the following criteria (other log types have similar filtering criteria):

- Start date and time
- End date and time
- Protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP)
- Virus name
- Action (delete, quarantine, quarantine e-mail, block e-mail, and log)
- User name
- Client IP address
- Server IP address
- Recipient e-mail address
- URL or subject

To query and download logs:

1. Select **Monitoring > Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Logs Query** submenu tab. The Logs Query screen displays (see [Figure 6-11 on page 6-24](#)).

Depending on the selection that you make from the Log Type pull-down menu, the screen adjusts to display the settings for the selected type of log. [Figure 6-11 on page 6-24](#) displays the Virus log information settings as an example.

The screenshot displays the 'Log Query' settings page in the ProSecure Web/Email Security Threat Management (STM) Appliance interface. The page is titled 'Settings' and includes a 'help' icon. The main content area is divided into several sections:

- Select Log Type:** A dropdown menu for 'Log Type' is set to 'Virus'.
- View All:** A radio button option.
- Search Criteria:**
 - Start Date/Time:** 2009 - 08 - 16 05 : 40
 - End Date/Time:** 2009 - 08 - 16 05 : 40
 - Protocols:** Checkboxes for SMTP, POP3, IMAP, HTTP, FTP, and HTTPS.
 - Virus Name:** An empty text input field.
 - Action:** Checkboxes for Delete, Quarantine, Quarantine email, Block email, and Log.
 - User:** An empty text input field.
 - Client IP:** Four empty input boxes for IP address.
 - Server IP:** Four empty input boxes for IP address.
 - Recipient Email:** An empty text input field.
 - URL/Subject:** An empty text input field.
- Display:** A dropdown menu set to '15' entries per page.
- Select File Format to Download Log (zipped):** Radio buttons for 'CSV' (selected) and 'HTML'.

At the bottom of the form, there are two yellow buttons: 'Search' and 'Download'.

Figure 6-11

3. Select the checkboxes and radio buttons, make your selections from the pull-down menus, and complete the fields as explained in [Table 6-9 on page 6-25](#).

Table 6-9. Log Query Settings

Setting	Description (or Subfield and Description)
Log Type	Select one of the following log types from the pull-down menu: <ul style="list-style-type: none"> • Traffic. All scanned incoming and outgoing traffic. • Virus. All intercepted viruses. • Spyware. All intercepted spyware. • Spam. All intercepted spam, including spam that was detected through the blacklist, real-time blacklist, and Distributed Spam Analysis. • Email filters. All e-mails that are intercepted because of keyword, file type, file name, password, or size limit violations. • Content filters. All Web sites, URLs, and FTP sites that are intercepted because of Web category, blacklist, file type, or size limit violations. • System. The system event logs that include all system errors, informational messages, configuration changes, and system software updates. • Application. All intercepted application access violations.
View All	Select one of the following radio buttons: <ul style="list-style-type: none"> • View All. Display or download the entire selected log. • Search Criteria. Query the selected log by configuring the search criteria that are available for the selected log.
Search Criteria	Start Date/Time <p>From the pull-down menus, select the year, month, day, hours, and minutes for the start date and time.</p> <p>This field is available for the following logs: Traffic, Virus, Spyware, Spam, Email filters, Content filters, System, and Application.</p>
	End Date/Time <p>From the pull-down menus, select the year, month, day, hours, and minutes for the end date and time.</p> <p>This field is available for the following logs: Traffic, Virus, Spyware, Spam, Email filters, Content filters, System, and Application.</p>
	Protocols <p>Select one or more checkboxes to specify the protocols that are queried.</p> <p>The following protocols can be selected:</p> <ul style="list-style-type: none"> • For Traffic, Virus, and Spyware logs: SMTP, POP3, IMAP, HTTP, FTP, and HTTPS. • For the Spam log: SMTP and POP3. • For the Email filters log: SMTP, POP3, and IMAP. • For the Content filters log: HTTP, FTP, and HTTPS.
	User <p>The user name that is queried.</p> <p>This field is available for the following logs: Traffic, Virus, Spyware, Spam, Email filters, Content filters, and Application.</p>

Table 6-9. Log Query Settings (continued)

Setting	Description (or Subfield and Description)	
Search Criteria (continued)	Client IP	The client IP address that is queried. This field is available for the following logs: Traffic, Virus, Spyware, Spam, Content filters, and Application.
	Server IP	The server IP address that is queried. This field is available for the following logs: Traffic, Virus , Spyware, Content filters, and Application.
	Reason	Select one or more checkboxes to specify the reasons that are queried: The following reasons can be selected: <ul style="list-style-type: none"> • For the Email filters log: keyword, file type, file name, password, and size limit. • For the Content filters log: Web category, file type, blacklist, and size limit.
	Virus Name	The name of the virus that is queried. This field is available only for the Virus log.
	Spyware Name	The name of the spyware that is queried. This field is available only for the Spyware log.
	Action	Select one or more checkboxes to specify the malware treatment actions that are queried. The following actions can be selected: <ul style="list-style-type: none"> • For the Virus and Spyware logs: delete, quarantine, quarantine email, block email, or log. • For the Spam log: block, tag, or quarantine.
	Detected By	Select one or both checkboxes to specify the method by which spam is detected: Blacklist or Distributed Spam Analysis. This field is available only for the Spam log.
	Subject	The e-mail subject that is queried: This field is available for the following logs: Spam and Email filters.
	Sender Email	The e-mail address of the sender that is queried. This field is available only for the Traffic log.
	Recipient Email	The e-mail address of the recipient that is queried. This field is available for the following logs: Traffic, Virus, Spyware, Spam, and Email filters.
	URL/Subject	The URL and subject that are queried. This field is available for the following logs: Traffic, Virus, and Spyware.

Table 6-9. Log Query Settings (continued)

Setting	Description (or Subfield and Description)	
Search Criteria (continued)	URL	The URL that is queried. This field is available only for the Content filters log.
	Category	The Web or application category that is queried. This field is available for the following logs: Content filters and Application.
	Size	The file's minimum and maximum size (in bytes) that are queried. This field is available only for the Traffic log.
	Type	Select one or more checkboxes to specify the system event types that are queried: error (all system errors), info (all informational messages), conf. (all configuration changes), and update (all system software updates). This field is available only for the System log.
	Event	The description of the event incident that is queried. This field is available only for the System log.
	Section	The application group (Instant Messaging, Media Applications, Peer to Peer, or Tools) that is queried. This field is available only for the Application log.
Display	The maximum number of pages that are displayed. The default setting is 15 entries.	
Download Log (zipped) File Format	Select a radio button to specify the format to download the zipped log file: <ul style="list-style-type: none"> • CSV. Download the log file as a comma separated values (CSV) file. • HTML. Download the log file as an HTML file. 	

4. Click one of the following action buttons:

- **Search.** Query the log according to the search criteria that you specified and view the log through the Web Management Interface, that is, on screen.
- **Download.** Query the log according to the search criteria that you specified and download the log to a computer.

Example: Using Logs to Identify Infected Clients

You can use the STM logs to help identify potentially infected clients on the network. For example, clients that are generating abnormally high volumes of HTTP traffic might be infected with spyware or a virus.

To identify infected clients that are sending spyware or a virus in outbound traffic, query the STM spyware and virus logs and see if any of your internal IP addresses are the source of spyware or a virus:

1. On the Log Query screen (see [Figure 6-11 on page 6-24](#)), select **Traffic** as the log type.
2. Select the start date and time from the pull-down menus.
3. Select the end date and time from the pull-down menus.
4. Next to Protocols, select the **HTTP** checkbox.
5. Click **Search**. After a while, the log appears on screen.
6. Check if there are clients that are sending out suspicious volumes of data, especially to the same destination IP address, on a regular basis.

If you find a client exhibiting this behavior, you can run a query on that client's HTTP traffic activities to get more information. Do so by running the same HTTP traffic query and entering the client IP address in the Client IP field.

Log Management

Generated logs take up space and resources on the STM internal disk. To ensure that there is always sufficient space to save newer logs, the STM automatically deletes older logs whenever the total log size reaches 50% of the allocated file size for each log type.

Automated log purging means that you do not need to constantly manage the size of the STM logs and ensures that the latest malware incidents and traffic activities are always recorded.



Note: The STM saves its logs every 5 minutes. If a power failure affects the STM, logs that were created within the 5-minute period before the power failure occurred are lost. Therefore, NETGEAR recommends that you connect the STM to a syslog server to save the logs externally.

To manually purge selected logs, see [“Clearing Logs” on page 6-7](#).

Scheduling and Generating Reports

The STM lets you schedule and generate four types of reports:

- **Email Reports.** For each protocol (SMTP, POP3, and IMAP), the report shows, the following information per day, both in tables and graphics:
 - Number of connections
 - Traffic amount in MB

- Number of malware incidents
- Number of files blocked
- Number of blacklist violations (not applicable to IMAP)
- Number of e-mails captured by Distributed Spam Analysis (not applicable to IMAP)
- **Web Reports.** The report shows the following information:
 - For each protocol (HTTP HTTPS, and FTP), the report shows the following information per day, both in tables and graphics:
 - Number of connections
 - Traffic amount in MB
 - Number of malware incidents
 - Number of files blocked
 - Number of URLs blocked (not applicable to FTP)
 - Top 10 blocked Web categories by count
- **System Reports.** The report shows malware incidents, CPU usage, and memory usage:
 - The following e-mail malware incident are shown, in tables:
 - For each protocol (SMTP, POP3, and IMAP), the number of detected malware incidents per day
 - Top 10 malware incidents by count
 - Top 10 infected clients by count
 - The following Web malware incident are shown, in tables:
 - For each protocol (HTTP HTTPS, and FTP), the number of detected malware incidents per day
 - Top 10 malware incidents by count
 - Top 10 infected clients by count
 - The CPU usage per day in percentage, in a graphic
 - The memory usage per day in percentage, in a graphic
- **Application Reports.** The report shows the following information:
 - The following application incidents are shown per day, in a table:
 - For each of the six Instant Messaging applications, the number of blocked requests
 - For each of the five Media applications, the number of blocked requests
 - For each of the four Tools applications, the number of blocked requests
 - For each of the three Peer to Peer applications, the number of blocked requests

- Top 10 blocked clients by count
- For each application, the number of blocked requests, in a graphic

The reports that you select are generated as MHTML files, which contain headers for the tables and graphics. You can download the reports as zipped files.

Generating Reports

To generate a report:

1. Select **Monitoring > Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Generate Report** submenu tab. The Generate Report screen displays.

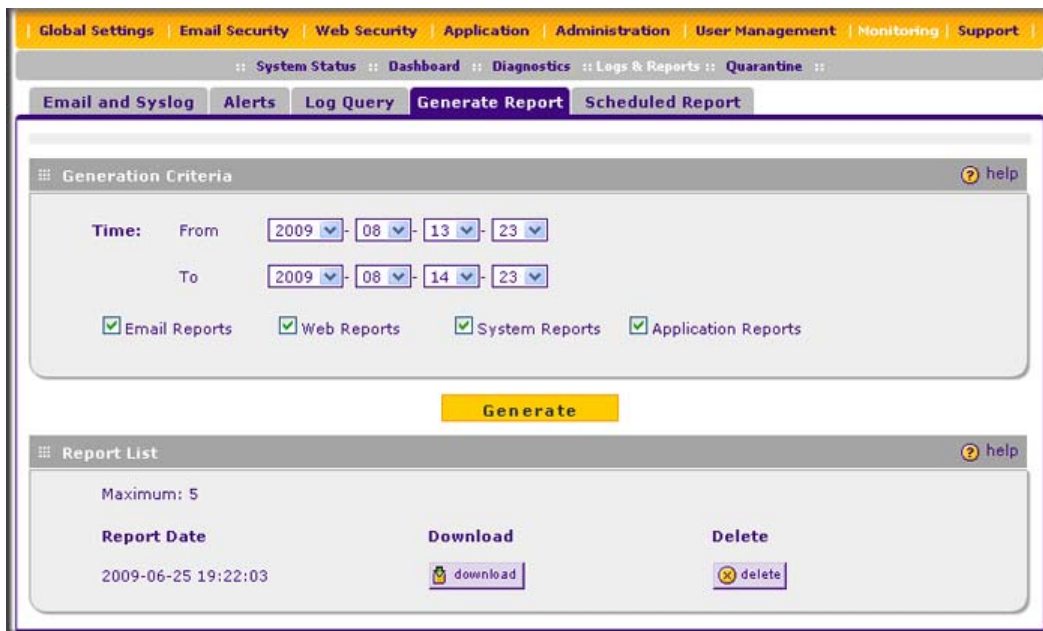


Figure 6-12

3. Make your selections from the pull-down menus and select the checkboxes as explained in [Table 6-10 on page 6-31](#).

Table 6-10. Generate Report Settings

Setting	Description
Time From	From the pull-down menus, specify the start year, month, day, hour, and minutes for the report.
Time To	From the pull-down menus, specify the end year, month, day, hour, and minutes for the report. Note: The maximum report period is 31 days.
Reports	Select one or more checkboxes to specify the reports that are generated: <ul style="list-style-type: none"> • Email Reports. • Web Reports. • System Reports. • Application Reports. Note: You can select all four checkboxes, but you might generate a very large report.

4. Click **Generate**. After a few minutes, the report are added to the Report List, which can contain a maximum of five saved reports. (To delete a a previously saved report, click its **delete** table button.)
5. Select the new or a previously saved report for downloading by clicking its **download** table button.

The report downloads as a zipped file that contains HTML files.

Scheduling Reports

To schedule automatic generation and e-mailing of reports:

1. Select **Monitoring > Logs & Reports** from the menu. The Logs & Reports submenu tabs appear, with the Email and Syslog screen in view.
2. Click the **Schedule Report** submenu tab. The Schedule Report screen displays (see [Figure 6-13 on page 6-32](#)).

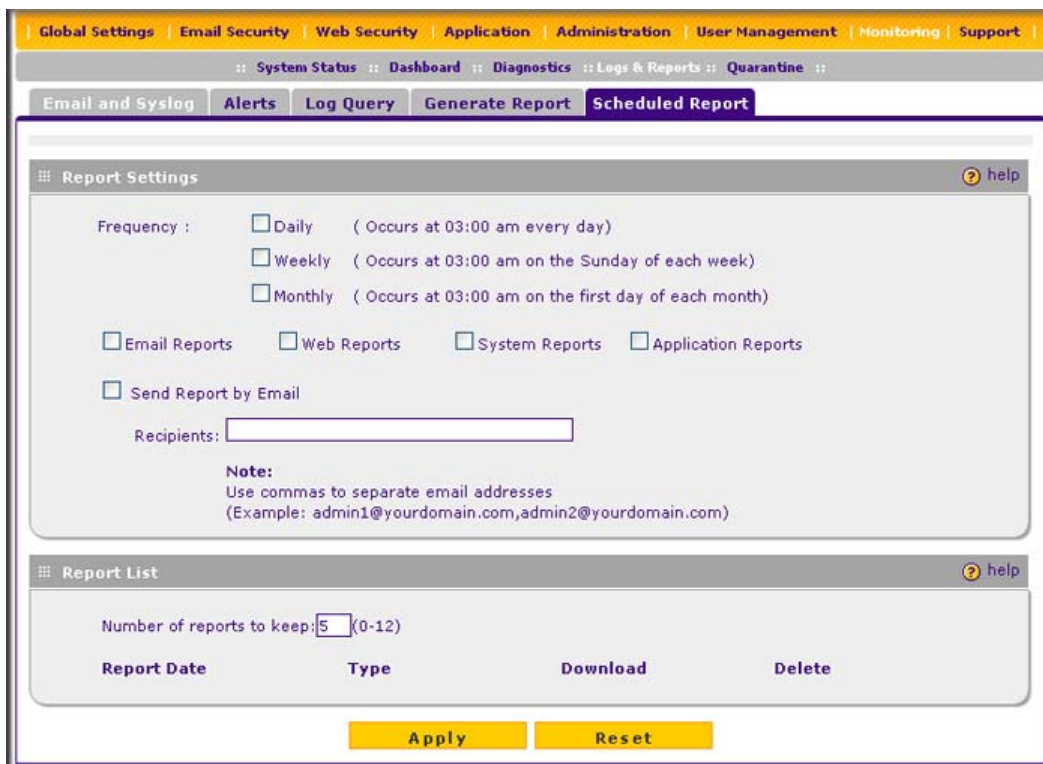


Figure 6-13

3. Select the checkboxes and complete the fields as explained in Table 6-11.

Table 6-11. Schedule Report Settings

Setting	Description
Report Settings	
Frequency	Select one of the following checkboxes to specify the frequency with which the reports are generated and e-mailed. <ul style="list-style-type: none"> • Daily. The report is generated daily at 3:00 am. • Weekly. The report is generated weekly on Sunday at 3:00 am. • Monthly. The report is generated monthly on first day of the month at 3:00 am.

Table 6-11. Schedule Report Settings (continued)

Setting	Description		
Reports	Select one or more checkboxes to specify the reports that are generated: <ul style="list-style-type: none"> • Email Reports. • Web Reports. • System Reports. • Application Reports. Note: You can select all four checkboxes, but you might generate a very large report.		
Send Report by Email	Select this checkbox to enable the STM to send the report to the recipients that you must specify below.		
	<table border="1"> <tr> <td>Recipients</td> <td>The e-mail addresses of the report recipients. Note: Use commas to separate e-mail addresses.</td> </tr> </table>	Recipients	The e-mail addresses of the report recipients. Note: Use commas to separate e-mail addresses.
Recipients	The e-mail addresses of the report recipients. Note: Use commas to separate e-mail addresses.		
Report List			
Number of Reports to Keep	Enter the number of reports that the STM saves. The maximum number is 12.		

- Click **Apply** to save your settings.

Viewing and Managing the Quarantine Files

Depending on the selections that you made in the Email Security and Web Security main menus (see [Chapter 4, “Content Filtering and Optimizing Scans](#)), the STM intercepts and saves e-mails that are infected by spam and both e-mails and files that are infected by malware threats (viruses and spyware) to its quarantine files. You can search these files, view the search results through the Web Management Interface, and then take a variety of actions that are described in [“Viewing and Managing the Quarantined Spam Table” on page 6-36](#) and [“Viewing and Managing the Quarantined Infected Files Table” on page 6-38](#). You can also specify how many entries are displayed per page (the default setting is 15 entries).



Note: To specify the quarantine settings, see [“Managing the Quarantine Settings” on page 3-30](#).

You can query and view the spam quarantine file and the malware quarantine file separately and filter the information based on a number of criteria. You can filter the spam quarantine file using the following criteria:

- Start date and time
- End date and time
- User name
- Source IP address
- Sender e-mail address
- Recipient e-mail address
- Subject
- Size of the e-mail

You can filter the malware quarantine file using the following criteria:

- Start date and time
- End date and time
- Protocols (HTTP, HTTPS, FTP, SMTP, POP3, and IMAP)
- User name
- Malware name
- Client IP address
- Recipient e-mail address
- Recipient e-mail address
- URL or subject
- Size of the file

To query the quarantine files:

1. Select **Monitoring > Quarantine** from the menu. The Quarantine screen displays (see [Figure 6-14 on page 6-35](#)).
2. Depending on the selection that you make from the Quarantine File Type pull-down menu, the screen adjusts to display the settings for the selected type of quarantine file. [Figure 6-14 on page 6-35](#) displays the spam quarantine file settings as an example.

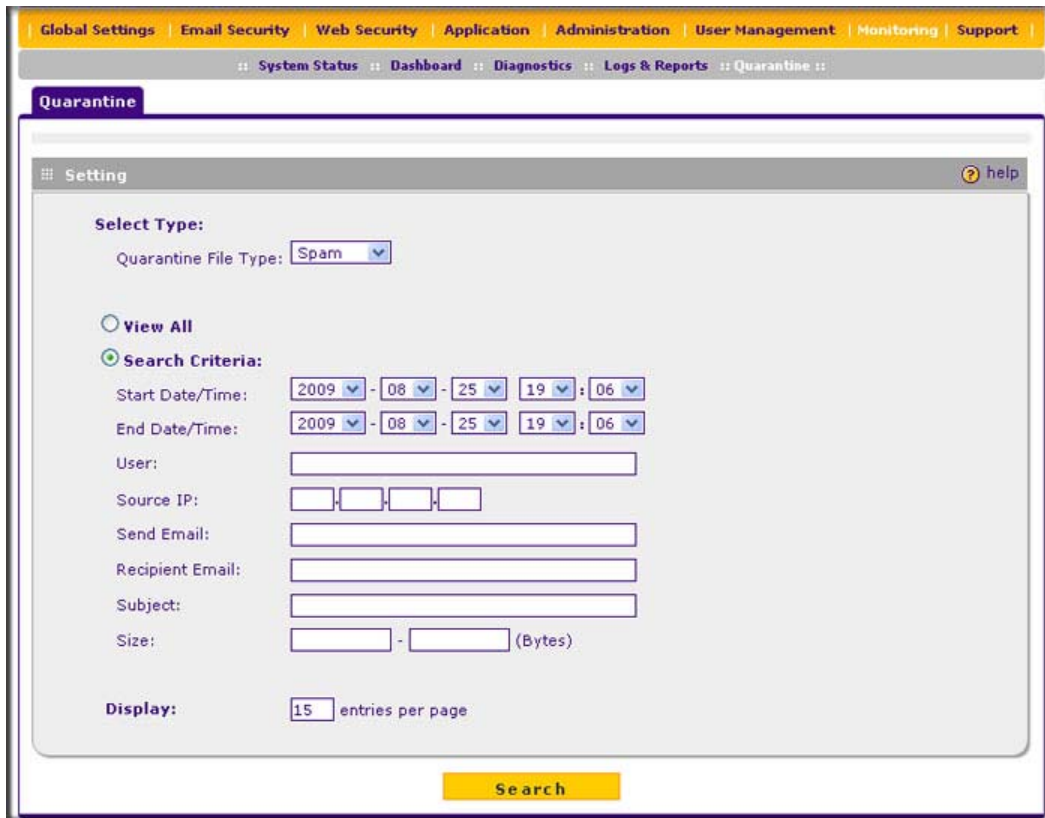


Figure 6-14

3. Select the checkboxes and radio buttons, make your selections from the pull-down menus, and complete the fields as explained in Table 6-9.

Table 6-12. Quarantine File Settings

Setting	Description (or Subfield and Description)
File Type	Select one of the following file types from the pull-down menu: <ul style="list-style-type: none"> • Spam. Quarantined spam that was detected through Distributed Spam Analysis. • Malware. All quarantined spyware and viruses.
View All	Select one of the following radio buttons: <ul style="list-style-type: none"> • View All. Display or download the entire selected quarantine file. • Search Criteria. Query the selected quarantine file by configuring the search criteria that are available for the selected file.
Search Criteria	

Table 6-12. Quarantine File Settings (continued)

Setting	Description (or Subfield and Description)	
Search Criteria (continued)	Start Date/Time	From the pull-down menus, select the year, month, day, hours, and minutes for the start date and time.
	End Date/Time	From the pull-down menus, select the year, month, day, hours, and minutes for the end date and time.
	Protocols	Select one or more checkboxes to specify the protocols that are queried (malware quarantine file only).
	User	The user name that is queried.
	Malware Name	The name of the spyware or virus that is queried (malware quarantine file only).
	Client IP	The client IP address that is queried (malware quarantine file only).
	Source IP	The source IP address that is queried (spam quarantine file only).
	Sender Email	The e-mail address of the sender that is queried (spam quarantine file only).
	Recipient Email	The e-mail address of the recipient that is queried.
	URL/Subject	The URL or subject that is queried (malware quarantine file only).
	Subject	The subject that is queried (spam quarantine file only).
	Size	The file's minimum and maximum size (in bytes) that are queried.
Display	The maximum number of pages that are displayed. The default setting is 15 entries.	

4. Click **Search**. Depending on the selected quarantine file (spam or malware), the Quarantine screen displays the Quarantined Spam table or the Quarantined Infected Files table, which are explained in the following sections.

Viewing and Managing the Quarantined Spam Table

When you query the spam quarantine file, the Quarantine screen with the Quarantined Spam table displays (see [Figure 6-15 on page 6-37](#)).



Figure 6-15

The Quarantined Spam table shows the following columns:

- **Checkbox.** Lets you select the table entry.
- **Date.** The date that the e-mail was received.
- **Protocol.** The protocol (SMTP) in which the spam was found.
- **User.** The user name that was used to log on the STM.
- **Client IP.** The client IP address from which the spam originated.
- **From.** The e-mail address of the sender.
- **To.** The e-mail address of the recipient.
- **Subject.** The e-mail subject line.
- **Size (Bytes).** The size of the e-mail in bytes.

Figure 6-16 show the Quarantined Spam table with data.

<input type="checkbox"/>	Date	Protocol	User	Client IP	From	To	Subject	Size(Byte)
<input type="checkbox"/>	2009-08-27 09:54:27	SMTP	anonymous	10.40.2.107	zjpop3@test.com	zjimap@test.com	testpppppp	2079
<input type="checkbox"/>	2009-08-27 09:54:20	SMTP	anonymous	10.40.2.107	zjpop3@test.com	zjimap@test.com	tttt	1869

Figure 6-16

After you have selected one or more table entries, take one of the following actions (or click the **Return** hyperlink to return to the previous screen):

- **Send as Spam.** The selected spam e-mail files are tagged as spam for Distributed Spam Analysis, and are sent to the intended recipients.

- **Send as Ham.** The selected spam e-mail files are not tagged as spam for Distributed Spam Analysis, are deleted from the quarantine file, and are sent to the intended recipients.
- **Delete.** The selected spam e-mail files are deleted from the quarantine file.

Viewing and Managing the Quarantined Infected Files Table

When you query the malware quarantine file, the Quarantine screen with the Quarantined Infected Files table displays (see [Figure 6-17](#)).



Figure 6-17

The Quarantined Infected Files table shows the following columns:

- **Checkbox.** Lets you select the table entry.
- **Date.** The date that the file was received.
- **Protocol.** The protocol (SMTP, POP3, IMAP, HTTP, FTP, HTTPS) in which the spyware or virus was found.
- **User.** The user name that was used to log on the STM.
- **Malware name.** The name of the spyware or virus.
- **File name.** The name of the file in which the spyware or virus was found.
- **Client IP.** The client IP address from which the spyware or virus originated.
- **Server IP.** The server IP address from which the spyware or virus originated.
- **From.** The e-mail address of the sender.
- **To.** The e-mail address of the recipient.
- **URL/Subject.** The URL or subject that is associated with the spyware or virus.
- **Size (Bytes).** The size of the virus or spyware file in bytes.

Figure 6-18 shows the Quarantined Infected Files table with data.

<input type="checkbox"/>	Date	Protocol	User	Malware Name	Filename	Client IP	Server IP	From	To	URL/Subject	Size(Bytes)
<input type="checkbox"/>	2009-08-26 03:20:40	SMTP	anonymous	EICAR-Test-File	附件 virus1.rar	10.40.2.107	10.40.2.63	zjpop3@test.com	zjmap@test.com	哈哈aa	17576
<input type="checkbox"/>	2009-08-25 10:14:21	SMTP	anonymous	Trojan-Spy.Win32.KeyLogger.s	spyware[1].sample.VIR	10.40.2.107	10.40.2.63	zjpop3@test.com	zjmap@test.com	test3	7168
<input type="checkbox"/>	2009-08-25 10:13:46	SMTP	anonymous	EICAR-Test-File	virus1.rar	10.40.2.107	10.40.2.63	zjpop3@test.com	zjmap@test.com	test2	17576

Figure 6-18

After you have selected one or more table entries, take one of the following actions (or click the **Return** hyperlink to return to the previous screen):

- **Resend to Admin.** The selected malware files are deleted from the quarantine file, zipped together as an e-mail attachment, and then send to the recipient that you have specified on the Email Notification Server server screen (see [“Configuring the E-mail Notification Server” on page 6-2](#)).
- **Delete.** The selected malware files are deleted from the quarantine file.

User-Generated Spam Reports

Users logging in through the User Portal Login screen can select to receive a report with intercepted spam e-mails that were intended for their e-mail address.

To send a spam report to an e-mail address, a user should do the following:

1. On the User Portal Login screen (see [Figure 5-7 on page 5-10](#)), click the “here” hyperlink in the “Check your quarantined mail here” section. The Send Spam Report screen displays. (see [Figure 6-19](#), which shows the STM600).

The screenshot shows the 'Send Spam Report' interface. At the top, there is a purple header with the 'NETGEAR PROSECURE' logo and the text 'NETGEAR ProSecure Web/Email Security Threat Management Appliance STM600'. Below the header is a yellow bar. The main content area is a white box with a grey border. It contains a 'Send Spam Report' title and a 'help' link. The 'Begin Date/Time' field is set to 2009-08-25 00:00. The 'Send to:' field is empty. A yellow 'Send Report' button is located to the right of the 'Send to:' field. At the bottom of the screen, there is a copyright notice: '2009 © Copyright NETGEAR ©'.

Figure 6-19

2. Select the start date and time from the Begin Date/Time pull-down menus.
3. Specify the recipient's e-mail address in the Send to field.



Note: The report includes only quarantined spam e-mails that contain the e-mail address that is specified in the Send to field.

4. Click **Send Report**.



Note: The report provides summary information such as time, sender, recipient, subject, and size, and a retrieve link. The user can retrieve an individual e-mail by clicking the retrieve link for the e-mail.

Using Diagnostics Utilities

The STM provides diagnostic tools that help you analyze traffic conditions and the status of the network. Two sets of tools are available:

- **Network diagnostic tools.** These tools include a ping utility, traceroute utility, and DNS lookup utility.
- **Traffic diagnostic tools.** These tools allow you to perform real-time, per-protocol traffic analysis between specific source and destination addresses and let you generate reports on network usage in your network.



Note: For normal operation, diagnostic tools are not required.

To display the Diagnostics screen, select **Monitoring > Diagnostics** from the menu. To facilitate the explanation of the tools, the Diagnostics screen is divided and presented in this manual in three figures ([Figure 6-20 on page 6-41](#), [Figure 6-21 on page 6-42](#), and [Figure 6-22 on page 6-43](#)).

Using the Network Diagnostic Tools

This section discusses the Ping or Trace an IP Address section and the Perform a DNS Lookup section of the Diagnostics screen.

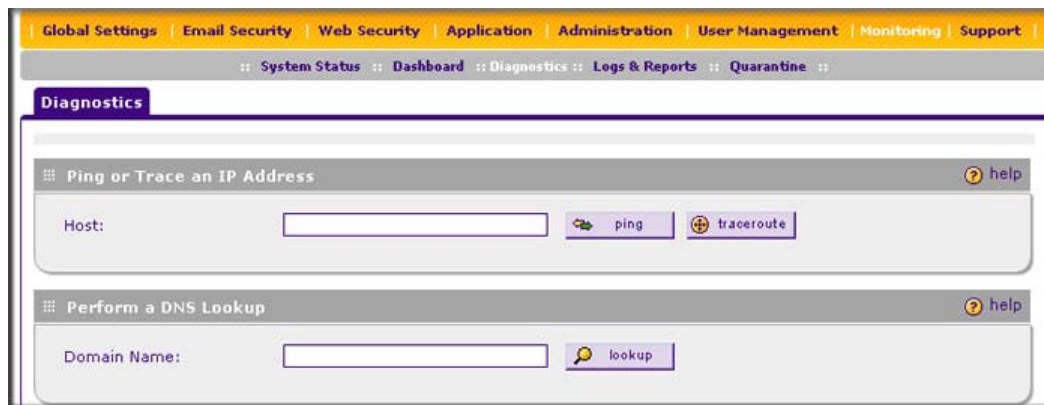


Figure 6-20 [Diagnostics, screen 1 of 3]

Sending a Ping Packet

Use the Ping utility to send a ping packet request in order to check the connection between the STM and a specific IP address. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results are displayed on a new screen; click “Back” on the Windows menu bar to return to the Diagnostics screen.

To send a ping:

1. Locate the Ping or Trace an IP Address section on the Diagnostics screen.
2. In the Host field, enter the IP address or host name that you want to ping.
3. Click the **ping** button. The results of the ping are displayed below the Host field.

Tracing a Route

A traceroute lists all routers between the source (the STM) and the destination IP address.

To send a traceroute:

1. Locate the Ping or Trace an IP Address section on the Diagnostics screen.
2. In the Host field, enter the IP address or host name for which you want trace the route.
3. Click the **traceroute** button. The results of the traceroute are displayed below the Host field.

Looking up a DNS Address

A DNS (Domain Name Server) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, mail, or other server on the Internet, request a DNS lookup to find the IP address.

To look up a DNS address:

1. Locate the Perform a DNS Lookup section on the Diagnostics screen.
2. In the Domain Name field, enter a domain name.
3. Click the **lookup** button. The results of the lookup action are displayed are displayed below the Domain Name field

Using the Realtime Traffic Diagnostics Tool

This section discusses the Realtime Traffic Diagnostics section and the Perform a DNS Lookup section of the Diagnostics screen.

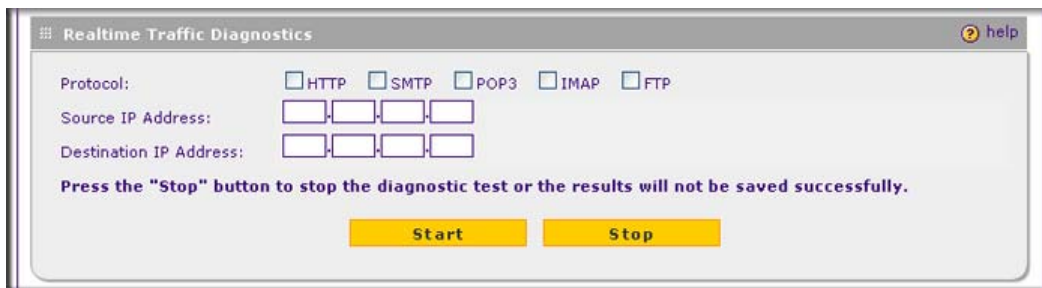


Figure 6-21 [Diagnostics, screen 2 of 3]

You can use the Realtime Traffic Diagnostics tool to analyze traffic patterns with a network traffic analyzer tool. Depending on the network traffic analyzer tool that you use, you can find out which applications are using most bandwidth, which users use most bandwidth, how long users are connected, and other information.

To use the Realtime Traffic Diagnostics tool:

1. Locate the Realtime Traffic Diagnostics section on the Diagnostics screen.
2. Select one or more checkboxes to specify the protocols for which you want to capture the traffic flow. The checkboxes that you can select are **HTTP**, **SMTP**, **POP3**, **IMAP**, and **FTP**.
3. In the Source IP Address field, enter the IP address of source of the traffic stream that you want to analyze.

4. In Destination IP Address, enter the IP address of the destination of the traffic stream that you want to analyze.
5. Click **Start**. You are prompted to save the downloaded traffic information file to your computer, however, do not save the file until you have stopped capturing the traffic flow.
6. When you want to stop capturing the traffic flow, click **Stop**.
7. Select a location to save the captured traffic flow. (The default file name is diagnostics.result.dat.) The file downloads to the location that you specify.
8. When the download is complete, browse to the download location you specified and verify that the file has been downloaded successfully.
9. Send the file to NETGEAR Technical Support for analysis.

Gathering Important Log Information and Generating a Network Statistics Report

When you request support, NETGEAR Technical Support might ask you to collect the debug logs and other information from your STM.

This section discusses the Gather Important Log Information section, Network Statistics Report section, and Reboot the System section of the Diagnostics screen.

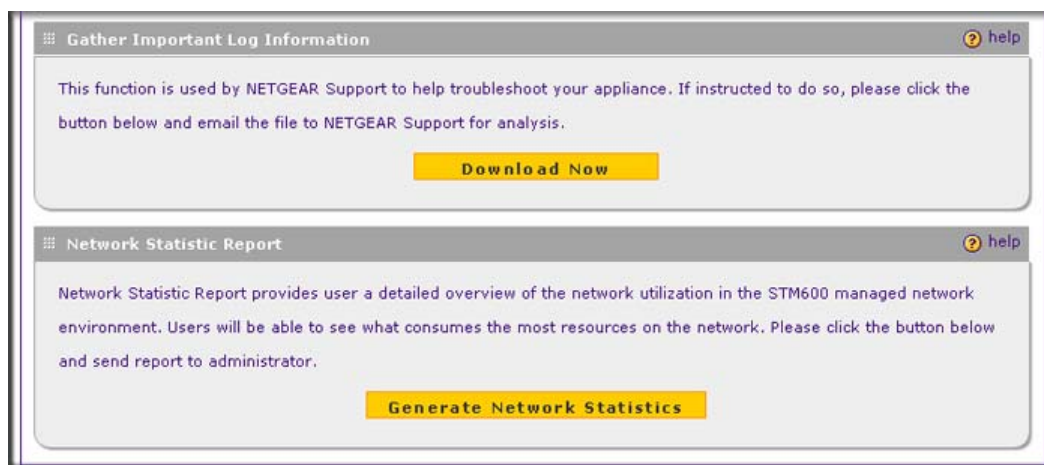


Figure 6-22 [Diagnostics, screen 3 of 3]

Gathering Important Log Information

To gather log information about your STM:

1. Locate the Gather Important Log Information section on the Diagnostics screen.
2. Click **Download Now**. You are prompted to save the downloaded log information file to your computer. The default file name is importantlog.gpg.
3. When the download is complete, browse to the download location you specified and verify that the file has been downloaded successfully.

Generating Network Statistics

The Network Statistic Report provides a detailed overview of the network utilization in the STM managed network environment. The report allows you to see what consumes the most resources on the network.

To generate the Network Statistic Report:

1. Locate the Network Statistics Report section on the Diagnostics screen.
2. Click **Generate Network Statistics**. The Network Statistic Report is sent in an e-mail to the recipient that you have configured on the E-mail Notification Server screen (see [“Configuring the E-mail Notification Server”](#) on page 6-2).

Restarting and Shutting Down the STM

You can perform a remote restart, for example, when the STM seems to have become unstable or is not operating normally.



Note: Restarting breaks any existing connections either to the STM (such as your management session) or through the STM (for example, LAN users accessing the Internet). However, connections to the Internet are automatically re-established when possible.

To restart the STM:

1. Locate the Restart & Shutdown section on the Diagnostics screen (this section is not shown on any of the Diagnostics screen figures in this manual).
2. Click the **Restart** button. The STM restarts. (If you can see the unit: the reboot process is complete when the Test LED on the front panel goes off.)



Note: See also [“Updating the Software”](#) on page 3-19.



Note: For the STM150 only, there is an alternate way to restart: press the Power button on the rear panel of the STM150 (see [“Rear Panel STM150”](#) on page 1-14). The front panel Test LED flashes, and the STM150 reboots.

To shut down the STM:

1. Locate the Restart & Shutdown section on the Diagnostics screen (this section is not shown on any of the Diagnostics screen figures in this manual).
2. Click the **Shutdown** button. The STM shuts down.



Note: You can shut down the STM using the Web Management Interface, but you cannot start up the STM using the Web Management Interface.

Chapter 7

Troubleshooting and Using Online Support

This chapter provides troubleshooting tips and information for the STM. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the STM on?
Go to [“Basic Functioning”](#) on page 7-2.
- Have I connected the STM correctly?
Go to [“Basic Functioning”](#) on page 7-2.
- I cannot access the STM’s Web Management Interface.
Go to [“Troubleshooting the Web Management Interface”](#) on page 7-3.
- A time-out occurs.
Go to [“When You Enter a URL or IP Address a Time-out Error Occurs”](#) on page 7-4.
- I have problems with the LAN connection.
Go to [“Troubleshooting a TCP/IP Network Using a Ping Utility”](#) on page 7-5.
- I want to clear the configuration and start over again.
Go to [“Restoring the Default Configuration and Password”](#) on page 7-6
- The date or time is not correct.
Go to [“Problems with Date and Time”](#) on page 7-7
- I need help from NETGEAR.
Go to [“Using Online Support”](#) on page 7-8.



Note: The STM’s diagnostic tools are explained in [“Using Diagnostics Utilities”](#) on page 6-40.

Basic Functioning

After you turn on power to the STM, the following sequence of events should occur:

1. When power is first applied, verify that the PWR LED is on.
2. After approximately two minutes, verify that:
 - a. The Test LED (STM150) or Status LED (STM300 and STM600) is no longer lit.
 - b. The LAN port Left LEDs are lit for any local ports that are connected.
 - c. The WAN port Left LEDs are lit for any WAN ports that are connected.

If a port's Left LED is lit, a link has been established to the connected device. If a port is connected, verify the following Right LED behavior in relation to the established port speed:

- Connected to a 1000-Mbps device:
 - STM150: The Right LED is green.
 - STM300: The Right LED is amber.
 - STM600: The Right LED is amber.
- Connected to a 100-Mbps device:
 - STM150: The Right LED is amber.
 - STM300: The Right LED is green.
 - STM600: The Right LED is green.
- Connected to a 10-Mbps device: for all STM models, the Right LED is off.

If any of these conditions do not occur, see the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your STM is turned on, make sure that the power cord is properly connected to your STM and that the power supply adapter is properly connected to a functioning power outlet. If the error persists, you have a hardware problem and should contact NETGEAR Technical Support.

Test LED or Status LED Never Turns Off

When the STM is powered on, the Test LED (STM150) or Status LED (STM300 and STM600) turns on for approximately 2 minutes and then turns off when the STM has completed its initialization. If the Test LED (STM150) or Status LED (STM300 and STM600) remains on, there is a fault within the STM.

If all LEDs are still more than several minutes after power up:

- Turn the power off, and then turn it on again to see if the STM recovers.
- Clear the STM's configuration to factory defaults. Doing so sets the STM's IP address to **192.168.1.201**. This procedure is explained in [“Restoring the Default Configuration and Password” on page 7-6](#).

If the error persists, you might have a hardware problem and should contact NETGEAR Technical Support.

LAN or WAN Port LEDs Not On

If either the LAN LEDs or WAN LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the STM and at the hub, router, or workstation.
- Make sure that power is turned on to the connected hub, router, or workstation.
- Be sure you are using the correct cables:

When connecting the STM's uplink (WAN) ports to one or two devices that provide the Internet connections, use the cables that are supplied with the devices. These cables could be a standard straight-through Ethernet cables or an Ethernet crossover cables.

Troubleshooting the Web Management Interface

If you are unable to access the STM's Web Management Interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the STM as described in the previous section ([“LAN or WAN Port LEDs Not On](#)).
- If your STM's IP address has been changed and you do not know the current IP address, clear the STM's configuration to factory defaults. This sets the STM's IP address to **192.168.1.201**. This procedure is explained in [“Restoring the Default Configuration and Password” on page 7-6](#).



Tip: If you do not want to revert to the factory default settings and lose your configuration settings, you can restart the STM and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the STM's LAN interface address.

- Make sure that you are using the SSL `https://address` login rather than the `http://address` login.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that Caps Lock is off when entering this information.

If the STM does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the Apply button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

When You Enter a URL or IP Address a Time-out Error Occurs

A number of things could be causing this situation. Try the following troubleshooting steps.

- Check whether other computers on the LAN work properly. If they do, ensure that your computer's TCP/IP settings are correct.
- If the computer is configured correctly, but still not working, ensure that the STM is connected and turned on. Connect to the Web Management Interface and check the STM's settings. If you cannot connect to the STM, see the information in the previous section ([“Troubleshooting the Web Management Interface” on page 7-3](#)).
- If the STM is configured correctly, check your Internet connection (for example, your modem or router) to make sure that it is working correctly.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the Ping utility in your PC or workstation.

Testing the LAN Path to Your STM

You can ping the STM from your PC to verify that the LAN path to the STM is set up correctly.

To ping the STM from a PC running Windows 95 or later:

1. From the Windows toolbar, click **Start** and choose **Run**.
2. In the field provided, type “ping” followed by the IP address of the STM; for example:

```
ping 192.168.1.201
```

3. Click **OK**. A message, similar to the following, should display:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you will see this message:

```
Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you will see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
 - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in [“LAN or WAN Port LEDs Not On” on page 7-3](#).
 - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and STM.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
 - Verify that the IP address for your STM and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

where <IP address> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your STM listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel.
- Check to see that the network address of your PC (the portion of the IP address that is specified by the netmask) is different from the network address of the remote device.
- Check that the modem or router is connected and functioning.

Restoring the Default Configuration and Password

To reset the STM to its original factory default settings:

1. Select **Administration > Backup and Restore Settings** from the menu. The Backup and Restore Settings screen displays.

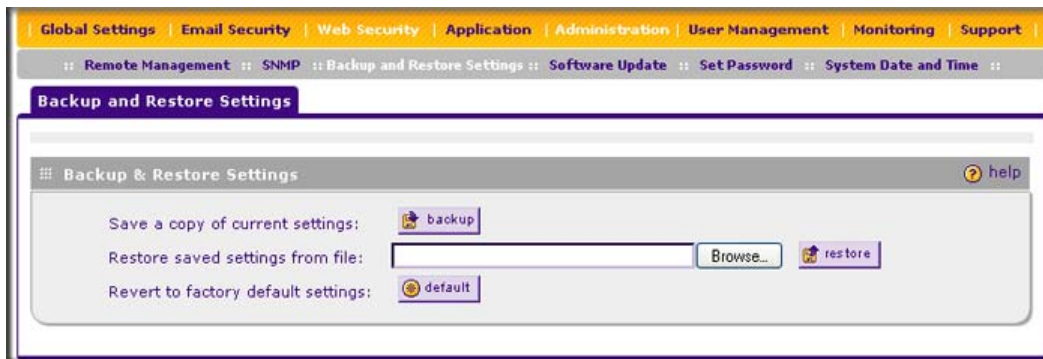


Figure 7-1

2. Next to Revert to factory default settings, click the **default** button.

The STM restarts. During the reboot process, the Backup & Restore Settings screen remains visible. The reboot process is complete after several minutes when the Test LED (STM150) or Status LED (STM300 and STM600) on the front panel goes off.



Warning: When you restore the factory default settings, the STM settings are erased. All scan and anti-spam settings are lost. Back up your settings if you intend on using them.



Note: After rebooting with factory default settings, the STM administrator account password is **password**, the guest account password is **guest**, and the LAN IP address is **192.168.1.201**.



Note: For the STM150 only, there is an alternate way to return the settings to factory default: using a sharp object, press and hold the Reset button on the rear panel of the STM150 (see [“Rear Panel STM150” on page 1-14](#)) for about 10 seconds until the front panel Test LED flashes and the STM150 returns to factory default settings.

Problems with Date and Time

The System Date and Time screen displays the current date and time of day (see [“Configuring Date and Time Service” on page 3-23](#)). The STM uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The STM has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the STM, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The STM does not automatically sense Daylight Savings Time. Check the Time Zone menu, and select or deselect the checkbox marked “Adjust for Daylight Savings Time”.

Using Online Support

The STM includes online support tools that allow NETGEAR Technical Support to securely perform diagnostics of the STM, and that lets you submit suspicious files for analysis by NETGEAR. You can also access the knowledge base and documentation online.

Enabling Remote Troubleshooting

One of the advanced features that the STM provides is online support through a support tunnel. With this feature, NETGEAR Technical Support staff is able to analyze from a remote location any difficulty you might be experiencing with the STM and to perform advanced diagnostics. Make sure that ports 443 and 2222 are open on your firewall, and that you have the support key that was given to you by NETGEAR.

To initiate the support tunnel:

1. Select **Support > Online Support** from the menu. The Online Support screen displays.

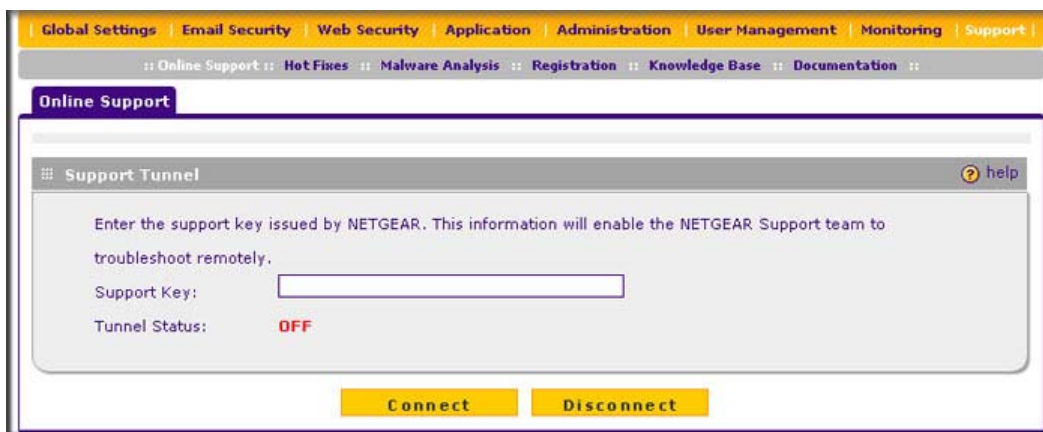


Figure 7-2

2. In the Support Key field, enter the support key that was given to you by NETGEAR
3. Click **Connect**. When the tunnel is established, the tunnel status field displays ON.

To terminate the tunnel, click **Disconnect**. The tunnel status field displays OFF.

If NETGEAR Technical Support cannot access the STM remotely, they might ask you to save a log file to your computer and then e-mail it to NETGEAR for analysis (see [“Gathering Important Log Information and Generating a Network Statistics Report”](#) on page 6-43).

Installing Hot Fixes

NETGEAR might release hot fixes or patches if certain problems are found in any software release. When a hot fix is available, install it immediately to ensure optimum performance of the STM. Hot fixes might be released through NETGEAR resellers or might be available on the NETGEAR ProSecure Web site at <http://prosecure.netgear.com>.

To display information about installed hot fixes, select **Support > Hot Fixes** from the menu. The Hot Fixes screen displays.

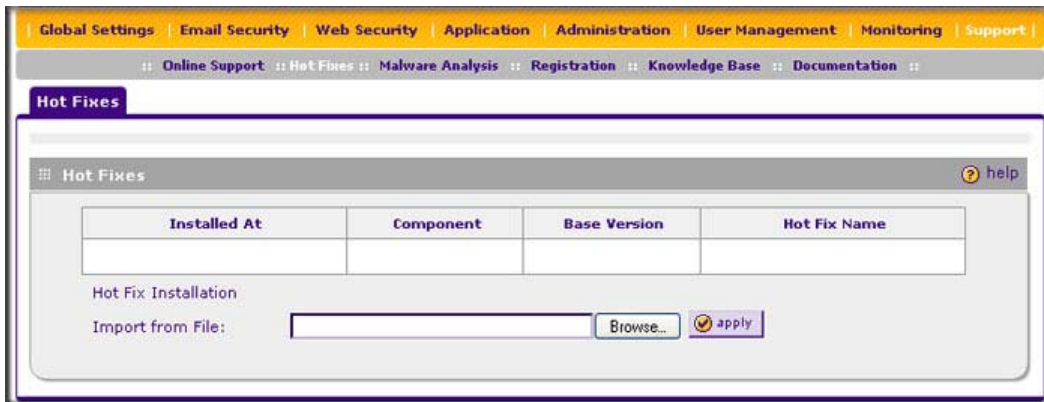


Figure 7-3

The Hot Fixes table displays the installed hot fixes with the following fields:

- **Installed At.** The date and time when the hot fix was installed on the STM.
- **Component.** The component for which the hot fix provides a patch.
- **Base Version.** The base software version for the hot fix. The hot fix cannot be installed on an earlier or later software version, but only on the software version for which it is intended.
- **Hot Fix Name.** The name of the hot fix.

To install a hot fix:

1. Obtain the hot fix from NETGEAR or its authorized reseller.
2. Save the hot fix file on the computer that you will use to access the STM.
3. Log in to the STM.
4. Select **Support > Hot Fixes** from the menu. The Hot Fixes screen displays (see [Figure 7-3](#)).
5. Next to the Import from File field, click **Browse**.

6. Navigate to the location on your computer where you have saved the hot fix file, and then select it.
7. Click Open. The hot fix file now appears in the Import from File field.
8. Click **Apply** to install the hot fix.

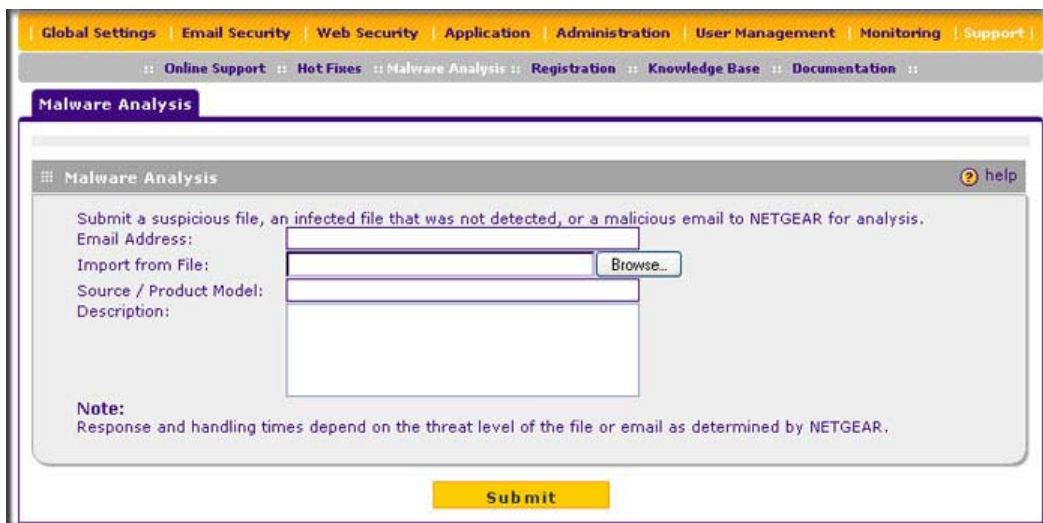
The Test LED (STM150) or Status LED (STM300 and STM600) blinks during the hot fix installation.

Sending Suspicious Files to NETGEAR for Analysis

You can report any undetected malware file or malicious e-mail to NETGEAR for online for analysis. The file is compressed and password-protected before it is sent.

To submit a file to NETGEAR for analysis:

1. Select **Support > Malware Analysis** from the menu The Online Support screen displays.



The screenshot shows a web browser window with a navigation menu at the top containing: Global Settings | Email Security | Web Security | Application | Administration | User Management | Monitoring | Support. Below the menu is a breadcrumb trail: :: Online Support :: Hot Fixes :: Malware Analysis :: Registration :: Knowledge Base :: Documentation ::. The main content area is titled "Malware Analysis" and contains the following text: "Submit a suspicious file, an infected file that was not detected, or a malicious email to NETGEAR for analysis." Below this text are four input fields: "Email Address:" (text box), "Import from File:" (text box with a "Browse..." button), "Source / Product Model:" (text box), and "Description:" (text area). At the bottom of the form is a yellow "Submit" button. A "Note:" section at the bottom of the form reads: "Response and handling times depend on the threat level of the file or email as determined by NETGEAR."

Figure 7-4

2. Complete the fields as explained in [Table 7-1](#) on page 7-11.

Table 7-1. Malware Analysis Settings

Setting	Description
Email Address	The e-mail address of the submitter to enable NETGEAR to contact the submitter if needed.
File Location	Click Browse to navigate to the file that you want to submit to NETGEAR.
Source / Product Model	Specify where the file originated (for example, an e-mail address if received via e-mail) and, if known, which product or scan feature (for example, the UTM or a desktop anti virus application) detected the file.
Description	As an option, include a description or any information that is relevant.

3. Click **Submit**.

Accessing the Knowledge Base and Documentation

To access NETGEAR's Knowledge Base for the STM, select **Support > Knowledge Base** from the menu.

To access NETGEAR's documentation library for your STM model, select **Support > Documentation** from the menu.

Appendix A

Default Settings and Technical Specifications

To return the STM returns to the default factory configuration settings that are shown in [Table A-1](#), click the **default** button on the Backup and Restore Settings screen (see [“Reverting to Factory Default Settings”](#) on page 3-18).

Table A-1. STM Default Configuration Settings

Feature	Default
Login	
User Login URL	https://192.168.1.201
Admin User Name (case-sensitive)	admin
Admin Login Password (case-sensitive)	password
Guest User Name (case-sensitive)	guest
Guest Login Password (case-sensitive)	guest
Management	
System Configuration	Web-based configuration and status monitoring
Required Minimum Browser versions	Microsoft Internet Explorer 5.1 or higher Mozilla Firefox 1.x or higher Apple Safari 1.2 or higher Note: When the unit scans secure HTTPS traffic, you must import the root CA certificate into your browser from the STM login screen.
Time Zone	GMT (Greenwich Mean Time)
Time Adjusted for Daylight Savings Time	Enabled
SNMP	Disabled
Administration Console Port	RS232

Table A-1. STM Default Configuration Settings (continued)

Feature	Default
LAN Connections	
MAC Address	Default address
MTU Size	1500
Ports	STM150: 5 AutoSense 10/100/1000BASE-T, RJ-45 STM300: 3 AutoSense 10/100/1000BASE-T, RJ-45 STM600: 5 AutoSense 10/100/1000BASE-T, RJ-45
LAN IP Address	In line transparent bridged
Subnet Mask	255.255.255.0

Table A-2 shows the STM specifications.

Table A-2. STM Specifications

Feature	Specification
Supported Protocols	
Data Protocols	HTTP, HTTPS, FTP, IMAP, POP3, SMTP
Power	
Worldwide	100–240V AC/50–60 Hz, universal input, 1.5 A max
Physical Specifications	
Dimensions (H x L x W)	STM150: 43.5 x 258 x 440 mm (1.7 x 10.2 x 17.3 in.) STM300: 44.4 x 500 x 426 mm (1.75 x 19.7 x 16.8 in.) STM600: 44.4 x 500 x 426 mm (1.75 x 19.7 x 16.8 in.)
Weight	STM150: 3.68 kg (8.1 lb.) STM300: 8.2 kg (18.1 lb.) STM600: 8.2 kg (18.1 lb.)
Form Factor	1U
Environmental Specifications	
Operating temperature	0° to 40° C (32° to 104° F)
Storage temperature	–20° to 70° C (–4° to 70° F)
Operating humidity	5–95% maximum relative humidity, noncondensing
Meets requirements of	RoHS

Table A-2. STM Specifications (continued)

Feature	Specification
Electromagnetic Emissions	
	Meets requirements of FCC Part 15 Class A VCCI Class A CE mark, commercial
Safety	
	Meets requirements of UL listed C-Tick

Appendix B Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document Link	Link
TCP/IP Networking Basics	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Networking Basics	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing Your Network	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking Basics	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm

Numerics

10BaseT, 100BaseT, and 1000BaseT [3-4](#)

A

AC input

STM150 [1-14](#)

STM300 [1-15](#)

STM600 [1-15](#)

access

preventing inherited privileges [5-11](#)

read/write and read-only [3-9](#)

remote management [3-11](#)

action buttons (Web Management Interface) [2-8](#)

activating, service licenses [1-6, 2-28](#)

Active Directory (AD)

domains [5-16](#)

how it works [5-12](#)

overview [5-11](#)

ActiveX objects [4-3](#)

administrator (admin)

overview [3-9](#)

receiving

alerts by e-mail [6-8](#)

logs by e-mail [6-4](#)

reports by e-mail [6-33](#)

settings [3-10](#)

airflow [1-17](#)

alerts

e-mail address for sending alerts [6-2](#)

specifying alerts to send via e-mail [6-8](#)

Alexa Toolbar [4-3, 4-46](#)

allowing

e-mails [4-17](#)

URLs [4-34](#)

Web

access exceptions [4-49](#)

categories [2-25, 4-30](#)

anti-spam settings, backing up [3-16](#)

anti-virus

action if infected e-mails [2-15](#)

user notification settings [4-10](#)

application software, updating [3-19](#)

applications

control [4-44](#)

logs [6-5, 6-6, 6-22, 6-25](#)

recent 5 and top 5 violations [6-15](#)

reports [6-29, 6-33](#)

setting access exceptions [4-52](#)

status [6-13](#)

attached devices, monitoring with SNMP [3-13](#)

audio and video files

e-mail filtering [4-14](#)

FTP filtering [4-43](#)

Web filtering [4-30](#)

authenticated users [4-50](#)

authentication methods [5-11](#)

Auto Uplink [1-4](#)

autosensing, speed [3-4](#)

B

backing up, settings [3-16, 3-17](#)

BitTorrent [4-2, 4-46](#)

blacklist

e-mails [4-15](#)

URLs [4-34](#)

blocking

e-mails [4-17](#)

file extensions [4-11, 4-14, 4-26, 4-30, 4-43](#)

file names [4-11, 4-14](#)

- keywords, e-mails [4-11, 4-13](#)
- sites, reducing traffic [3-32](#)
- URLs [4-34](#)
- Web
 - access exceptions [4-49](#)
 - categories [2-25, 4-26, 4-30](#)
 - objects [4-26, 4-30](#)
- bottom panel and label
 - STM150 [1-16](#)
 - STM300 [1-16](#)
 - STM600 [1-17](#)
- browsers, for Web Management Interface [2-5](#)
- bundle key, for registering [2-28](#)
- buttons (hardware)
 - power
 - STM150 [1-14](#)
 - STM300 [1-15](#)
 - STM600 [1-15](#)
 - reset (STM150 only) [1-14, 3-18](#)
- buttons (software)
 - action (Web Management Interface) [2-8](#)
 - help (Web Management Interface) [2-9](#)
 - table (Web Management Interface) [2-9](#)

C

- CA [3-25](#)
- cache, clearing Web categories [4-32](#)
- capabilities and features [1-3](#)
- card, service registration [1-6](#)
- categories, Web content [2-25, 4-30](#)
- certificates
 - 3rd party Web site [4-39](#)
 - authentication [4-36](#)
 - commercial CAs [3-25](#)
 - exchange [4-36](#)
 - managing [3-25](#)
 - NETGEAR default [3-27](#)
 - self-signed [3-25](#)
 - trusted [3-28](#)
 - untrusted [3-29](#)
 - warning messages [2-7, 3-13, 4-37](#)
- certification authority. *See* CA.
- Challenge Handshake Authentication Protocol. *See* RADIUS-CHAP.
- clearing statistics [6-11](#)
- clients, identifying infected [6-27](#)
- community strings, SNMP [3-15](#)
- community, ProSecure™ [xiv](#)
- comparison, STM models [1-5](#)
- compatibility, protocols [A-2](#)
- compliance, regulatory and safety [A-3](#)
- compressed files
 - e-mail filtering [4-14](#)
 - FTP filtering [4-43](#)
 - Web filtering [4-30](#)
- concurrent
 - number of users [1-5](#)
 - scanned HTTP connections [1-5](#)
- configuration
 - changes, system logs [6-5](#)
 - settings, defaults [A-1](#)
 - using the Setup Wizard [2-10](#)
- Configuration Manager Login [5-9](#)
- configuration menu (Web Management Interface) [2-8](#)
- connections, concurrently scanned, HTTP [1-5](#)
- console port
 - STM150 [1-14](#)
 - STM300 [1-10](#)
 - STM600 [1-12](#)
- content filtering
 - blocked Web page, user notification settings [4-31](#)
 - e-mails [4-11, 4-12](#)
 - logs [6-5, 6-6, 6-22, 6-25](#)
 - overview [4-1, 4-26](#)
 - scheduling [4-31](#)
 - See also* e-mails, *See also* Web.
 - settings, using the Setup Wizard [2-24](#)
 - Web [2-25, 4-30](#)
- control, applications [4-44](#)
- conventions, typographical [xiii](#)
- cookies [4-3](#)
- CPU usage [6-13](#)
- critical updates [3-22](#)
- crossover cable [1-4, 7-3](#)

D

date

- settings 2-13, 3-23, 3-24
- troubleshooting 7-7

daylight savings time 2-13, 3-24

debug logs 6-43

dedicated management VLAN port 1-6

defaults

configuration

- restoring 7-6
- settings A-1

content filtering settings 4-2

domains, for authentication 5-25

factory default settings, reverting to 3-18

IP address 2-11, 3-3

login time-out 2-7

NETGEAR certificate 3-27

password 2-6

subnet mask 2-12, 3-4

user name 2-6

deployment

rack mounting 1-18

scenarios

- choosing 2-1
- gateway 2-1
- segmented LAN 2-3
- server group 2-2

testing

- connectivity 2-27
- HTTP scanning 2-27

verifying 2-27

diagnostics

- overview 6-40
- ping utility 6-41

distinguished name. *See* LDAP, dn.

Distributed Spam Analysis 4-19, 4-20

DNS

- looking up an address 6-42
- server IP addresses 2-12, 3-4

documentation, online 7-11

documents, reference B-1

domains

- default 5-25
- LDAP and Active Directory (AD) 5-16

overview 5-1

RADIUS 5-19

trusted 4-26

Web access exceptions, applying to 4-49

downlink ports. *See* LAN, ports.

downloading, SSL certificate 2-7

dropped packets, session limit exceeded 3-7

duplex, settings 3-4

dust 1-17

E

eDonkey 4-2, 4-46

EICAR 2-28

electrical noise 1-17

e-mail notification server

- configuring manually 6-2
- settings, using the Setup Wizard 2-19
- SMTP server 2-20, 6-3

e-mails

anti-virus

- settings 2-15
- user notifications 4-10

attachments, sizes 2-16, 4-8

audio and video files, filtering 4-14

blocked, statistics 6-17

compressed files, filtering 4-14

content filtering 4-11, 4-12

defaults, content filtering and scan settings 4-2

Distributed Spam Analysis 4-19, 4-20

executable files, filtering 4-14

filter logs 6-5, 6-6, 6-22, 6-25

protection. *See* SMTP, POP3, or IMAP.

real-time blacklist 4-17

reports 6-28, 6-33

scanned, statistics 6-17

security settings, using the Setup Wizard 2-14

SMTP throughput (e-mails per hour) 1-5

spam protection, overview 4-14

traffic statistics 6-13

whitelist and blacklist 4-15

environmental specifications A-2

error, system logs 6-5

exceptions, Web access 4-48

exclusions, scanning [4-47](#)

executable files

 e-mail filtering [4-14](#)

 FTP filtering [4-43](#)

 Web filtering [4-30](#)

F

facilities, syslog server [6-7](#)

factory defaults

 login [1-15](#)

 service licenses, automatic retrieval [2-30](#)

 settings, reverting to [3-18](#)

failure bypass [1-6](#)

features and capabilities [1-3](#)

file extensions, blocking [4-11, 4-14, 4-26, 4-30, 4-43](#)

file names, blocking [4-11, 4-14](#)

File Transfer Protocol. *See* FTP.

files, suspicious [7-10](#)

firmware

 updating [3-19](#)

 versions [6-21](#)

fixes, "hot" [7-9](#)

Flash objects [4-3](#)

forum, ProSecure™ [xiv](#)

FQDN [3-12](#)

front panel

 STM150 [1-8](#)

 STM300 [1-10](#)

 STM600 [1-12](#)

FTP

 action, infected Web file or object [2-19](#)

 audio and video files, filtering [4-43](#)

 compressed files, filtering [4-43](#)

 default port [2-18, 4-23](#)

 enabling scanning [2-18, 4-23](#)

 executable files, filtering [4-43](#)

 files and objects, sizes [4-43](#)

fully qualified domain name. *See* FQDN.

G

gateway address [3-4](#)

Gnutella [4-2, 4-46](#)

Google Talk [4-2, 4-46](#)

GoToMyPC [4-3, 4-46](#)

groups

 by IP address and subnet, managing [5-5](#)

 by IP membership, authentication [4-51](#)

 by name, managing [5-3](#)

 local [4-50](#)

 membership [5-2](#)

 overview [5-1](#)

 Web access exceptions, applying to [4-49](#)

guest users [3-9, 3-10](#)

guidelines, performance and sizing [1-5](#)

H

hard disk usage [6-13](#)

Hard drive (HDD) LED

 STM150, not applicable

 STM300 [1-11](#)

 STM600 [1-13](#)

hardware

 serial number [6-21](#)

 STM150

 bottom panel and label [1-16](#)

 front panel [1-8](#)

 LEDs [1-9, 7-2, 7-3](#)

 rear panel [1-14](#)

 STM300

 bottom panel and label [1-16](#)

 front panel [1-10](#)

 LEDs [1-11, 7-2, 7-3](#)

 rear panel [1-15](#)

 STM600

 bottom panel and label [1-17](#)

 front panel [1-12](#)

 LEDs [1-13, 7-2, 7-3](#)

 rear panel [1-15](#)

help button (Web Management Interface) [2-9](#)

hosts

 security alerts [3-25](#)

 trusted

 importing [4-41](#)

 SNMP [3-15](#)

 specifying [4-39](#)

hot fixes [7-9](#)

HTML, scanning [4-25](#)

HTTP

action, infected Web file or object [2-18, 4-25](#)

concurrently scanned connections [1-5](#)

default port [2-17, 4-23](#)

enabling scanning [2-17, 4-23](#)

logging, traffic [4-30](#)

proxy settings

 configuring manually [3-8](#)

 using the Setup Wizard [2-23](#)

proxy, for HTTPS scanning [4-36, 4-39](#)

testing scanning [2-27](#)

trusted hosts [4-39](#)

HTTPS

action, infected Web file or object [2-18, 4-25](#)

default port [2-18, 4-23](#)

enabling scanning [2-18, 4-23](#)

managing certificates [3-26](#)

scanning process [4-36](#)

trusted hosts [4-39](#)

Hypertext Markup Language. *See* HTML.

Hypertext Transfer Protocol over Secure Socket Layer.
See HTTPS.

Hypertext Transfer Protocol. *See* HTTP.

I

ICMP time-out [3-7](#)

ICQ [4-2, 4-46](#)

IDS [1-1](#)

IETF [3-13](#)

IMAP

action, infected e-mails [2-16, 4-7](#)

default port [2-15, 4-5](#)

enabling scanning [2-15, 4-5](#)

file extension blocking [4-14](#)

file name blocking [4-14](#)

password-protected attachment blocking [4-13](#)

importing

 certificates [3-27](#)

 trusted certificates [3-29](#)

 trusted hosts [4-41](#)

informational messages, system logs [6-5](#)

initial configuration, Setup Wizard [2-10](#)

installation, steps [2-4](#)

instant messaging services

 configuring [4-46](#)

 defaults [4-2](#)

 statistics [6-13](#)

interfaces

 speed and duplex settings [3-4](#)

 statistics [6-17](#)

 status [6-21](#)

Internet Engineering Task Force. *See* IETF.

Internet Message Access Protocol. *See* IMAP.

Intrusion Detection Systems. *See* IDS.

Intrusion Prevention Systems. *See* IPS.

IP addresses

 DNS servers [2-12, 3-4](#)

 STM [2-11, 3-3](#)

 subnet mask, STM [2-12, 3-4](#)

IPS [1-1](#)

iTunes [4-2, 4-46](#)

J

Java objects [4-3](#)

Javascript [4-3, 4-30](#)

K

KDE (MIB browser) [3-15](#)

Kensington lock (STM150 only) [1-14](#)

key (bundle), for registering [2-28](#)

keywords, blocking in e-mails [4-11, 4-13](#)

kit, rack-mounting [1-18](#)

Knowledge Base [7-11](#)

L

LAN

 default settings [A-2](#)

 LEDs [7-3](#)

 STM150 [1-9](#)

 STM300 [1-11](#)

 STM600 [1-13](#)

- troubleshooting [7-2, 7-3](#)
 - ports
 - STM150 [1-8](#)
 - STM300 [1-10](#)
 - STM600 [1-12](#)
 - LDAP
 - binding a dn [5-12](#)
 - configuring a dn [5-17](#)
 - domains [5-16](#)
 - overview [5-11](#)
 - settings [5-17](#)
 - users and groups [4-51](#)
 - LEDs
 - Hard drive (HDD)
 - STM150, not applicable
 - STM300 [1-11](#)
 - STM600 [1-13](#)
 - LAN
 - STM150 [1-9](#)
 - STM300 [1-11](#)
 - STM600 [1-13](#)
 - locations
 - STM150 [1-8](#)
 - STM300 [1-10](#)
 - STM600 [1-12](#)
 - Power
 - STM150 [1-9](#)
 - STM300 [1-11](#)
 - STM600 [1-13](#)
 - Status
 - STM150, not applicable
 - STM300 [1-11](#)
 - STM600 [1-13](#)
 - stop blinking (Test LED, Status LED) [6-21](#)
 - Test (STM150 only) [1-9](#)
 - troubleshooting [7-2, 7-3](#)
 - WAN
 - port speed indicators [7-2](#)
 - STM150 [1-9](#)
 - STM300 [1-11](#)
 - STM600 [1-13](#)
 - license expiration alert [6-8](#)
 - licenses
 - activating [2-28](#)
 - expiration dates [6-21](#)
 - key [1-6](#)
 - lifetime, quarantine [3-31](#)
 - Lightweight Directory Access Protocol. *See* LDAP.
 - limits, sessions [3-6](#)
 - location, placement [1-17](#)
 - lock, Kensington (STM150 only) [1-14](#)
 - log information, diagnostics [6-44](#)
 - logging
 - administrator e-mailing options [6-4](#)
 - clearing [6-8](#)
 - e-mail address for sending logs [6-2](#)
 - management [6-28](#)
 - querying logs [6-22](#)
 - search criteria [6-25](#)
 - selecting logs [6-25](#)
 - specifying logs to send via e-mail [6-5](#)
 - syslog server [6-6](#)
 - logging out, users
 - all active [5-25](#)
 - preventing inherited access privileges [5-11](#)
 - login
 - default settings [A-1](#)
 - time-out
 - changing [3-9](#)
 - defaults [2-7](#)
 - looking up, DNS address [6-42](#)
- ## M
- main navigation menu (Web Management Interface) [2-8](#)
 - malware
 - alerts [6-8, 6-10](#)
 - blocked page, user notification settings [4-25](#)
 - detected, statistics [6-17](#)
 - infected files, viewing [6-38](#)
 - logs [6-5, 6-6](#)
 - outbreak alerts [6-8, 6-10](#)
 - quarantine area size [3-31](#)
 - quarantined
 - querying and viewing [6-34](#)
 - statistics [6-17](#)
 - recent 5 and top 5 threats [6-15](#)
 - management
 - default settings [A-1](#)

digital certificates [3-25](#)
 performance [3-31](#)

Management Information Base. *See* MIB.

management ports
 STM150, not applicable
 STM300 [1-10](#)
 STM600 [1-12](#)

maximum transmission unit. *See* MTU (settings).

media applications
 configuring [4-46](#)
 defaults [4-2](#)
 status [6-13](#)

memory usage [6-13](#)

menu descriptions [2-8](#)

MG-Soft MIB browser) [3-15](#)

MIB, and MIB browsers [3-15](#)

mIRC [4-2, 4-46](#)

misclassification, of URLs [4-32](#)

models, STM [1-5](#)

moisture [1-17](#)

MSN Messenger [4-2, 4-46](#)

MTU settings [2-12, 3-5](#)

N

name, system [2-11, 3-3](#)

NETGEAR Configuration Manager Login [5-9](#)

NETGEAR registration server [1-7](#)

Net-SNMP (Linux Text) (MIB browser) [3-15](#)

network
 diagnostic tools [6-40, 6-41](#)
 statistics report, diagnostics [6-44](#)

network settings
 backing up [3-16](#)
 configuring manually [3-1](#)
 using the Setup Wizard [2-11](#)

Network Time Protocol. *See* NTP.

notification settings (users)
 anti-virus [4-10](#)
 malware, blocked page [4-25](#)
 URLs, blocked [4-35](#)
 Web content filtering, blocked page [4-31](#)

NTP [3-23](#)
 servers, settings [2-13, 3-23, 3-24](#)
 troubleshooting [7-7](#)

O

online
 analysis, by NETGEAR [7-10](#)
 documentation [7-11](#)
 support [7-8](#)

operating system, updating [2-22, 3-19](#)

outbreak, malware
 alerts [6-8, 6-10](#)
 defining [6-10](#)

P

package contents, STM [1-7](#)

packets
 dropped, exceeding session limit [3-7](#)
 transmitted and received, statistics [6-17](#)

pair of ports [1-6](#)

Password Authentication Protocol. *See* RADIUS-PAP.

password-protected attachments [4-11, 4-13](#)

passwords
 changing [3-9](#)
 default [2-6](#)
 restoring [7-6](#)

pattern file
 signatures [2-22](#)
 updating [2-22, 3-19](#)

peer-to-peer (P2P) services
 configuring [4-46](#)
 defaults [4-2](#)
 status [6-13](#)

performance and sizing guidelines [1-5](#)

performance, management [3-31](#)

phishing [4-19](#)

physical specifications [A-2](#)

pinging
 checking connections [6-41](#)
 ping utility, diagnostics [6-41](#)
 troubleshooting TCP/IP [7-5](#)

placement, location [1-17](#)

polling interval [6-11](#)

POP3

action, infected e-mails [2-15, 4-7](#)

default port [2-15, 4-5](#)

Distributed Spam Analysis [4-20](#)

enabling scanning [2-15, 4-5](#)

file extension blocking [4-14](#)

file name blocking [4-14](#)

keyword blocking [4-13](#)

password-protected attachment blocking [4-13](#)

ports

console

STM150 [1-14](#)

STM300 [1-10](#)

STM600 [1-12](#)

LAN

speed [7-2](#)

STM150 [1-8](#)

STM300 [1-10](#)

STM600 [1-12](#)

locations

STM150 [1-8](#)

STM300 [1-10](#)

STM600 [1-12](#)

management

STM150, not applicable

STM300 [1-10](#)

STM600 [1-12](#)

WAN

STM150 [1-8](#)

STM300 [1-10](#)

STM600 [1-12](#)

Post Office Protocol 3. *See* POP3.

power button

STM150 [1-14](#)

STM300 [1-15](#)

STM600 [1-15](#)

Power LED

STM150 [1-9](#)

STM300 [1-11](#)

STM600 [1-13](#)

troubleshooting [7-2](#)

power receptacle

STM150 [1-14](#)

STM300 [1-15](#)

STM600 [1-15](#)

power specifications, adapter [A-2](#)

printing, this manual [xiv](#)

priorities, syslog server [6-7](#)

product updates [xiv](#)

ProSecure™ forum and community [xiv](#)

ProSecure™ Web/Email Security Threat Management Appliance STM150, STM300, or STM600 Installation Guide [2-4](#)

protocols

compatibilities [A-2](#)

Web [4-22](#)

proxies

for HTTPS scanning [4-36](#)

HTTP

configuring manually [3-8](#)

using the Setup Wizard [2-23](#)

scanning defaults [4-3](#)

Q

QQ [4-2, 4-46](#)

quarantine

infected files (malware), viewing [6-38](#)

search criteria [6-36](#)

settings [3-30](#)

spam e-mails, viewing [6-37](#)

viewing [6-33](#)

question mark icon (Web Management Interface) [2-9](#)

Quicktime [4-2, 4-46](#)

R

rack-mount kit [1-18](#)

RADIUS

domains [5-19](#)

overview [5-11](#)

RADIUS-CHAP [5-12, 5-21](#)

RADIUS-PAP [5-12, 5-21](#)

shared secrets [5-21](#)

users [4-51](#)

VLANs [5-23](#)

read/write access, read-only access [3-9](#)

Real Player [4-2, 4-46](#)

real-time
 protection, capabilities [1-4](#)
 traffic, diagnostics [6-42](#)

real-time blacklist (RBL), e-mails [4-17](#)

real-time clock. *See* RTC.

rear panel
 STM150 [1-14](#)
 STM300 [1-15](#)
 STM600 [1-15](#)

rebooting [6-44](#)

reducing traffic [3-32](#)

reference documents [B-1](#)

registering with NETGEAR [2-28](#)

registration
 information [1-7](#)
 server, NETGEAR [1-7](#)

regulatory compliance [A-3](#)

Remote Authentication Dial In User Service. *See* RADIUS.

remote management [3-11](#)
 access [3-11](#)
 configuration [3-12](#)

remote troubleshooting, enabling [7-8](#)

removing, embedded objects [4-30](#)

reports
 e-mail address for sending reports [6-2](#)
 generating [6-30](#)
 scheduling [6-31](#)
 selecting, for administrator e-mailing [6-33](#)
 user-generated spam report [6-39](#)
 Web usage [6-19](#)

reset button, STM150 (only) [1-14](#), [3-18](#)

restoring
 factory default settings [3-18](#)
 settings, from backup file [3-17](#)

Rhapsody [4-2](#), [4-46](#)

routes, tracing [6-41](#)

RTC [2-13](#), [3-24](#)

rules, Web access exceptions [4-48](#)

S

safety compliance [A-3](#)

scan engine
 capabilities [1-4](#)
 updating [2-22](#), [3-19](#)

scan settings, backing up [3-16](#)

scanning
 e-mail security settings [2-15](#)
 exclusions [4-47](#)
 HTML files [4-25](#)
 overview [4-1](#)
 size exceptions
 e-mail attachments [2-16](#), [4-8](#)
 FTP files and objects [4-43](#)
 Web files and objects [2-19](#), [4-25](#)
 Web security settings [2-17](#)

scheduling
 content filtering [4-31](#)
 reports [6-31](#)
 updates [2-22](#), [3-19](#)
 Web access exceptions [4-51](#)

search criteria
 logs [6-25](#)
 quarantine [6-36](#)

Secure Socket Layer. *See* SSL.

security
 alerts, trusted or untrusted hosts [3-25](#)
 subscription update settings
 configuring manually [3-19](#)
 using the Setup Wizard [2-21](#)

service licenses
 activating [2-28](#)
 automatic retrieval [2-30](#)
 expiration dates [6-21](#)
 trial period [2-28](#)

service registration card [1-6](#)

sessions
 expiration length [5-24](#)
 limits [3-6](#)
 time-out [3-11](#)

Setup Wizard, initial configuration [2-10](#)

severities, syslog [6-6](#)

shared secrets, RADIUS [5-21](#)

- shutting down [6-44](#)
- signatures, pattern file [2-22](#)
- Simple Mail Transfer Protocol. *See* SMTP.
- Simple Network Management Protocol. *See* SNMP.
- size, exceptions
 - e-mail attachments [2-16, 4-8](#)
 - FTP files and objects [4-43](#)
 - Web files and objects [2-19, 4-25](#)
- size, quarantine areas [3-31](#)
- sizing and performance, guidelines [1-5](#)
- SMTP
 - action, infected e-mails [2-15, 4-6](#)
 - default port [2-15, 4-5](#)
 - Distributed Spam Analysis [4-20](#)
 - enabling scanning [2-15, 4-5](#)
 - file extension blocking [4-14](#)
 - file name blocking [4-14](#)
 - keyword blocking [4-13](#)
 - password-protected attachments, blocking [4-13](#)
 - server for e-mail notification [2-20, 6-3](#)
 - throughput (e-mails per hours) [1-5](#)
- sniffer [7-4](#)
- SNMP
 - overview [3-13](#)
 - settings [3-14](#)
 - SNMPv1 and SNMPv2, supported [3-13](#)
 - traps [3-15](#)
 - trusted hosts [3-15](#)
- software updates, system logs [6-5](#)
- software, STM [2-22](#)
- spam
 - blocked messages, recent 5 and top 5 [6-15](#)
 - detected, statistics [6-17](#)
 - Distributed Spam Analysis [4-19](#)
 - logs [6-5, 6-6, 6-22, 6-25](#)
 - protection, overview [4-14](#)
 - quarantine area size [3-31](#)
 - quarantined
 - e-mails, viewing [6-37](#)
 - querying and viewing [6-34](#)
 - statistics [6-17](#)
 - real-time blacklist (RBL) [4-17](#)
 - reports, sending [4-21](#)
 - user-generated report [6-39](#)
 - whitelist and blacklist [4-15](#)
- Spamcop [4-18](#)
- Spamhaus [4-18](#)
- specifications, physical and technical [A-2](#)
- speed
 - autosensing [3-4](#)
 - settings [3-4](#)
- spyware
 - logs [6-22, 6-25](#)
 - See also* anti virus, *See also* e-mails.
- SSL
 - certificate
 - warning [4-37](#)
 - warning and downloading [2-7](#)
 - connection and HTTPS scanning [4-36](#)
 - encryption for LDAP [5-17](#)
 - warning message [3-13](#)
- statistics
 - interfaces [6-17](#)
 - service and traffic [6-17](#)
- status
 - interfaces [6-21](#)
 - Web Management Interface [6-21](#)
- Status LED
 - STM150, not applicable
 - STM300 [1-11](#)
 - STM600 [1-13](#)
 - stop blinking [6-21](#)
 - troubleshooting [7-2](#)
- status, system [6-13, 6-19](#)
- STM150 hardware
 - bottom panel and label [1-16](#)
 - front panel [1-8](#)
 - LEDs [1-9, 7-2, 7-3](#)
 - rear panel [1-14](#)
- STM300 hardware
 - bottom panel and label [1-16](#)
 - front panel [1-10](#)
 - LEDs [1-11, 7-2, 7-3](#)
 - rear panel [1-15](#)
- STM600 hardware
 - bottom panel and label [1-17](#)
 - front panel [1-12](#)
 - LEDs [1-13, 7-2, 7-3](#)

rear panel [1-15](#)

Stream Scanning technology overview [1-4](#)

streaming, scanned file parts [2-18, 4-25](#)

submenu tabs (Web Management Interface) [2-8](#)

subnet mask, STM [2-12, 3-4](#)

support, online [7-8](#)

suspicious files [7-10](#)

switch, power

- STM150 [1-14](#)
- STM300 [1-15](#)
- STM600 [1-15](#)

syslog server [6-6](#)

system

- date and time settings, using the Setup Wizard [2-12, 2-13](#)
- logs [6-5, 6-6, 6-22, 6-25](#)
- name [2-11, 3-3](#)
- reports [6-29, 6-33](#)
- status [6-13, 6-19](#)

T

table buttons (Web Management Interface) [2-9](#)

tabs, submenu (Web Management Interface) [2-8](#)

TCP time-out [3-7](#)

TCP/IP, network, troubleshooting [7-5](#)

technical specifications [A-2](#)

Test LED (STM150 only)

- description [1-9](#)
- stop blinking [6-21](#)
- troubleshooting [7-2](#)

testing

- connectivity [2-27](#)
- HTTP scanning [2-27](#)

throughput

- SMTP (e-mails per hour) [1-5](#)
- Web scan [1-5](#)

time

- daylight savings
 - applied automatically [2-13, 3-24](#)
 - troubleshooting [7-7](#)
- settings [2-13, 3-23, 3-24](#)
- troubleshooting [7-7](#)

- zone [2-13, 3-24](#)

time-out

- errors [7-4](#)
- sessions [3-11](#)
- TCP, UDP, and ICMP [3-7](#)

TLS [5-17](#)

tools (online)

- configuring [4-46](#)
- defaults [4-3](#)
- status [6-13](#)

tracing a route (traceroute) [6-41](#)

traffic

- diagnostic tools [6-40](#)
- logs [6-5, 6-6, 6-22, 6-25](#)
- real-time diagnostics [6-42](#)
- reducing [3-32](#)
- total scanned, in MB [6-17](#)
- total, in bytes [6-15](#)

Transport Layer Security. *See* TLS.

traps, SNMP [3-15](#)

trial period, service licenses [2-28](#)

troubleshooting

- basic functioning [7-2](#)
- browsers [7-4](#)
- configuration settings, using sniffer [7-4](#)
- defaults [7-4](#)
- LEDs [7-2, 7-3](#)
- NTP [7-7](#)
- remotely [7-8](#)
- testing your setup [7-6](#)
- time-out error [7-4](#)
- Web Management Interface [7-3](#)

trusted

- certificates [3-28](#)
- domains [4-26](#)
- hosts [4-39](#)
- URLs [4-27](#)

typographical conventions [xiii](#)

U

UDP time-out [3-7](#)

unauthenticated users [4-50](#)

untrusted certificates [3-29](#)

- update failure alert [6-8, 6-9](#)
- update servers [2-22, 3-21](#)
- update settings
 - backing up [3-16](#)
 - security subscriptions
 - configuring manually [3-19](#)
 - using the Setup Wizard [2-21](#)
- updates
 - critical [3-22](#)
 - product *xiv*
 - scheduling [2-22, 3-19](#)
- updating software
 - automatically [3-21](#)
 - manually [3-21](#)
 - overview [3-19](#)
- uplink ports. *See* WAN, ports.
- URLs
 - blacklist [4-34](#)
 - blocked
 - statistics [6-17](#)
 - user notification settings [4-35](#)
 - categorization [4-32](#)
 - misclassification [4-32](#)
 - settings access exceptions [4-52](#)
 - trusted [4-27](#)
 - using wildcards [4-34](#)
 - whitelist [4-34](#)
- USB port, non-functioning
 - STM150 [1-8](#)
 - STM300 [1-10](#)
 - STM600 [1-12](#)
- User Portal Login Link [5-9](#)
- users
 - accounts, configuring [5-6](#)
 - administrative (admin) [3-9, 3-10, 5-9](#)
 - authenticated [4-50, 5-2](#)
 - global settings [5-24](#)
 - guests [3-9, 3-10](#)
 - logging out [5-11](#)
 - number of concurrent [1-5](#)
 - overview [5-1](#)
 - searching [4-51, 5-26](#)
 - special privileges [5-9](#)
 - unauthenticated [4-50, 5-1](#)
 - Web access exceptions, applying to [4-49](#)

V

- virtual LAN. *See* VLAN(s).
- virus
 - logs [6-22, 6-25](#)
 - See also* malware.
- VLAN port, dedicated management [1-6](#)
- VLANs, using for authentication [5-23](#)

W

- WAN
 - LEDs [7-3](#)
 - port speed indicators [7-2](#)
 - STM150 [1-9](#)
 - STM300 [1-11](#)
 - STM600 [1-13](#)
 - troubleshooting [7-3](#)
 - ports
 - STM150 [1-8](#)
 - STM300 [1-10](#)
 - STM600 [1-12](#)
- warning message, SSL certificate [2-7, 3-13, 4-37](#)
- Weatherbug [4-3, 4-46](#)
- Web
 - audio and video files, filtering [4-30](#)
 - blocked URL, user notifications [4-35](#)
 - categories
 - blocked, recent 5 and top 5 [6-15](#)
 - blocking [2-25, 4-26, 4-30](#)
 - default settings [4-3](#)
 - filtering, using the Setup Wizard [2-24](#)
 - setting access exceptions [4-52](#)
 - compressed files, filtering [4-30](#)
 - content filtering
 - blocked page, user notifications [4-31](#)
 - logs [6-5, 6-6, 6-22, 6-25](#)
 - overview [4-26](#)
 - defaults, content filtering and scan settings [4-2](#)
 - executable files, filtering [4-30](#)
 - files and objects, sizes [2-19, 4-25](#)
 - malware, blocked page, user notifications [4-25](#)
 - objects
 - blocking [4-26, 4-30](#)
 - default settings [4-3](#)
 - protection. *See* HTTP, *See* HTTPS, *See* FTP.

- reports [6-29](#), [6-33](#)
- scan throughput [1-5](#)
- security settings, using the Setup Wizard [2-17](#)
- statistics [6-13](#)
- usage
 - monitoring [6-18](#)
 - reports [6-19](#)

Web Management Interface [2-8](#)

- browsers, qualified [2-5](#)
- layout [2-8](#)
- settings [2-11](#)
- status [6-21](#)
- troubleshooting [7-3](#)

whitelist

- e-mails [4-15](#)
- URLs [4-34](#)

wildcards, using for URLs [4-34](#)

Winamp [4-2](#), [4-46](#)

Y

Yahoo Messenger [4-2](#), [4-46](#)

Yahoo Toolbar [4-3](#), [4-46](#)

Z

zone, time [2-13](#), [3-24](#)

